Christine Albiani
Maria Clara Seixas
Organizadoras

ANAIS
II EDIÇÃO DO CONCURSO DE PAPERS SOBRE PROTEÇÃO DE DADOS PESSOAIS

FACULDADE BAIANA DE DIREITO
FACULDADE BAIANA DE DIREITO E GESTÃO

Editoração Eletrônica: Marília Borges
Capa: Marília Borges

Rua José Peroba, 123, Costa Azul, Salvador/BA. CEP: 41.770-235.
Tel: 3205-7744

publicacoes@faculdadebaianadedireito.com.br
http://www.faculdadebaianadedireito.com.br

C744 Concurso de Papers Sobre Proteção de Dados Pessoais (2. : 2024 : Salvador)
Anais II Edição do Concurso de Papers Sobre Proteção de Dados Pessoais / organizadoras Christine Albiani, Maria Clara Seixas. – Salvador : Faculdade Baiana de Direito, 2024.
59 p.

Bibliografia.
Publicação digital (e-book) no formato PDF.
ISBN 978-65-87051-11-6.

1. Proteção de Dados. 2. Direito a Privacidade. I. Título.

CDD 342.0858

Ficha catalográfica elaborada pelo Setor de Processamento da Faculdade Baiana de Direito.

SUMÁRIO

APRESENTAÇÃO

É com enorme satisfação que publicamos os Anais da 2º edição do Concurso de Papers sobre Proteção de Dados Pessoais da Faculdade Baiana de Direito. Foram meses de preparação para que o nosso alunado pudesse usufruir de um evento de alta qualidade técnica e organização.

Em sua 2ª edição, o Concurso de Papers teve como objetivo estimular as discussões sobre proteção e privacidade em nossa comunidade e a pesquisa e produção científica sobre o tema, como parte do Programa de Privacidade e Proteção de Dados da Faculdade Baiana de Direito e Gestão, dentro do pilar de conscientização e do fomento da cultura de privacidade na instituição.

Os trabalhos foram apresentados em formato de papers, um pequeno artigo científico, e avaliados pelas organizadoras Christine Albiani e Maria Clara Seixas, tendo sido apresentados durante o evento favorecendo o debate dos professores e alunos, um momento muito enriquecedor para todos os participantes.

Publicar os anais do 2º Concurso de Papers não apenas celebra o esforço e dedicação de todos os envolvidos, mas também abre portas para o aprofundamento contínuo do conhecimento e a troca de ideias sobre proteção de dados pessoais.

Os papers aqui reunidos representam valiosas contribuições científicas, que servirão de referência para futuras pesquisas e debates, beneficiando toda a comunidade acadêmica e profissional.

DADOS PESSOAIS E LGPD: UMA ANÁLISE ACERCA DO ARQUIVAMENTO DOS PRONTUÁRIOS MÉDICOS E O DEVER DO SIGILO

Luana Guimarães Santos Abramovitz[1]

RESUMO:

O presente trabalho se destina a analisar a aplicação da LGPD no arquivamento dos prontuários médicos e o dever de sigilo com relação aos dados pessoais sensíveis dos pacientes. A proposta discorre sobre o desenvolvimento do atendimento médico qualificado e a possibilidade de compilar dados pessoais sensíveis dos pacientes. A pesquisa visa esclarecer quais são os limites do sigilo médico com relação à necessidade de utilização do conteúdo dos prontuários. O estudo é bibliográfico e qualitativo e utilizou-se do método dedutivo.

Palavras chave: Dados pessoais sensíveis; LGPD; Prontuário médico; Sigilo médico.

1 INTRODUÇÃO

A presente pesquisa refere-se ao estudo do arquivamento de prontuários médicos que contém dados pessoais sensíveis de pacientes, em consonância com o dever de sigilo médico e com a aplicação da Lei Geral de Proteção de Dados (LGPD). Dessa forma, este artigo abordará as seguintes problemáticas: A quem pertence o prontuário médico? Quais os impactos da LGPD no arquivamento de dados sensíveis dos pacientes? Quais são os limites da aplicação do dever de sigilo médico?

1 Graduanda em Direito pela Faculdade Baiana de Direito.

Outrossim, é imperioso falar que a abordagem desse tema tem grande relevância social e jurídica, tendo em vista que, com o advento da tecnologia, os prontuários passaram a se configurar também como eletrônicos, intensificando o tratamento dos dados pessoais, sendo indissociável a veemente necessidade de estudar os aspectos de aplicação da LGPD nos processos de tratamento de dados pessoais dos documentos físicos e digitalizados.

Também é válido destacar que este trabalho enquadra-se em pesquisa bibliográfica, pois baseia-se em artigos de revistas, teses e dissertações de repositórios de diversas faculdades. Ademais, o estudo abarca uma pesquisa qualitativa, visto que através da interpretação e da avaliação do objeto de pesquisa construiu-se pontos relacionados aos problemas de pesquisa mencionados, que deram origem a diversos questionamentos acerca do tema.

Por fim, o presente artigo científico se baseia no método dedutivo hipotético para confirmar, através de doutrinas e hipóteses, as constatações presentes na tese de pesquisa, a fim de analisar a veracidade dos questionamentos formulados com base em premissas jurídicas.

2 PRONTUÁRIOS MÉDICOS E O DEVER DE SIGILO

Entende-se por prontuário médico não apenas o registro da anamnese do paciente, mas o acervo documental padronizado, organizado e conciso, referente ao registro dos cuidados médicos prestados. Este dossiê serve para a análise da evolução de doenças, para fins estatísticos e para a defesa do profissional, caso venha ser responsabilizado por algum resultado atípico ou indesejado (FRANÇA, 2013, p. 19).

Com a modernização dos sistemas de informação hospitalares que passavam a integrar dados clínicos e administrativos, foi necessária a modernização deste documento, dando origem aos primeiros prontuários eletrônicos na década de 70 (Lovis et al., 2011 apud SILVA, 2021, p. 2).

Uma questão relevante é a quem pertence o prontuário médico. O médico é, indubitavelmente, o autor intelectual do dossiê por ele recolhido, tendo o direito de guarda juntamente à instituição a quem presta seus serviços, mas é de propriedade do paciente a disponibilidade permanente das informações que possam ser objeto da sua necessidade de ordem pública ou privada (FRANÇA, 2013, p. 20).

Outra questão atinente ao tema é o sigilo médico, mais antigo e universal princípio da tradição médica que encontra-se no Juramento de Hipócrates

(FRANÇA, 2013, p. 132). Nesse sentido, todo paciente espera que as informações sejam mantidas como confidenciais, cabendo ao hospital manter a guarda desse sigilo. É necessário que haja autorização do paciente - ou de seu representante legal quando incapaz ou menor - por escrito, através de linguagem acessível e clara, para o uso das devidas informações por terceiros. Por outro lado, não existe exigência de autorização para manuseio interno do prontuário por servidores do hospital (FRANÇA, 2013, p. 141). No entanto, existem casos que ultrapassam o dever de sigilo médico: a) quando procede em decorrência de lei ou de solicitação judiciária, não podendo negar ao perito ou ao juiz tais documentos ou b) quando as consequências obriguem em favor da segurança e da saúde do paciente (FRANÇA, 2013, p. 145). Nessas situações, a revelação deve se limitar ao necessário, tendo o cuidado de indicar ao solicitante os objetivos e o limite de tempo da validade de tais dados.

Dessa forma, fica claro que a obrigação de guarda do segredo médico se estende aos prontuários e fichas hospitalares ou ambulatoriais e aqueles que não cumprirem tais fundamentos estão sujeitos às penas do art. 154 do Código Penal (FRANÇA, 2013, p. 145), que prevê detenção de três meses a um ano para aquele que revelar, sem justa causa, segredo de que tem ciência em razão de profissão, e cuja revelação possa produzir dano a outrem.

3 A APLICAÇÃO DA LGPD NO ARQUIVAMENTO DE DADOS PESSOAIS SENSÍVEIS

A LGPD, em seu art. 5º, considera como um dos tipos de dado pessoal sensível aquele referente à saúde e dado genético ou biométrico, quando vinculado a uma pessoa natural. Assim, é fato que o arquivamento do prontuário exige especial atenção, uma vez que eventual incidente de segurança com esses dados pode trazer consequências graves aos direitos de privacidade e intimidade dos titulares, tal como prevê o art. 17 deste dispositivo legal.

Outrossim, destaca-se que o art. 11 da LGPD possibilita que o tratamento de dados pessoais sensíveis ocorra nos casos de tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Esse dispositivo abrange a possibilidade de utilização dos dados contidos no prontuário médico para um atendimento qualificado.

Ocorre que alguns pacientes solicitam a entrega do prontuário médico por e-mail, prática que exige cuidados devido à falta de segurança, mas se estiver ciente do risco e demonstrar inequivocamente que o solicitante é o titular do direito da informação, não se verifica ilegalidade no envio pelo médico, vez que o sigilo é um direito do próprio paciente (CREMERS, 2021, p. 01). Nesse prisma, a legislação brasileira apresentou mudanças significativas no que

concerne ao prontuário eletrônico através da promulgação da Lei 13.787/18, que reúne diretrizes importantes sobre o tema e mantém determinações de algumas resoluções do Conselho Federal de Medicina (AGUIAR, 2021, p. 78).

Dessa forma, o art. 2° deste dispositivo legal aborda que o processo de digitalização do prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital, trazendo maior segurança ao manuseio de dados sensíveis. Outra inovação diz respeito aos prazos de eliminação dos prontuários, em que ambos, em papel ou digitalizados, deverão ser eliminados quando completados 20 anos a partir do último registro (AGUIAR, 2021, p. 86).

4 CONSIDERAÇÕES FINAIS

A partir do exposto, é fundamental discutir a aplicação de possíveis políticas de proteção de dados nas clínicas médicas, a fim de identificar e tratar os processos de forma que os dados coletados fiquem protegidos e disponíveis para quem possui autorização para consultá-los (Santos, Bahia, Lima, 2023, p. 179). Dessa forma, é importante que as clínicas visem investir em ações para a conscientização de funcionários, usuários, prestadores e pacientes, acerca da importância da proteção de dados pessoais sensíveis (Santos, Bahia, Lima, 2023, p. 181).

Além disso, para que a aplicação da LGPD seja bem-sucedida, as clínicas devem realizar um estudo interno para revisar as rotinas na coleta de dados e implementar instrumentos de proteção, visando obter o controle de acessos às informações e a salvaguarda dos bancos de dados, a fim de combater possíveis invasões, perda ou vazamento de informações. Outrossim, é interessante desenvolver projetos de proteção de dados com sistema de mitigação de riscos, emissão de relatórios e práticas de governança corporativa, além de revisar a forma de comunicação e troca de informações entre a empresa e os titulares de dados pessoais fornecidos (Santos, Bahia, Lima, 2023, p. 182).

Sendo assim, é inegável que as instituições de saúde devem estabelecer um critério definido do uso e da revelação dessas informações, de forma que se limitem sempre a fornecer o essencial e que se omitem ao máximo o acesso aos dados sensíveis de pacientes, mantendo-os como confidenciais (FRANÇA, 2013, p. 145).

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, Camila Nava. **Direito Médico: Estudo Teórico e Prático.** 05.ed. São Paulo: Editora Atena, 2021. Disponível em: https://atenaeditora.com.br/catalogo/ebook/direito-medico-estudo-teorico-e-pratico. Acesso em: 09 set. 2023.

BRASIL. **Lei 13.709**, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 set. 2023.

BRASIL. **Lei 13.787**, de 27 de dezembro de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 09 set. 2023.

CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO GRANDE DO SUL. **LGPD Regulamenta Entrega de Prontuário Médico ao Paciente**. 2021. Disponível em: https://cremers.org.br/lgpd-regulamenta-entrega-de-prontuario-medico-ao-paciente/. Acesso em: 08 set. 2023.

FRANÇA, Genival Veloso. **Direito Médico**. 11.ed. Rio de Janeiro: Editora Forense, 2013.

SANTOS, Fábio da Silva; BAHIA, Saulo José Casali; LIMA, Mario Jorge Philocreon de Castro. Aplicação da Lei Geral De Proteção De Dados (LGPD) nas Clínicas Médicas. **Direito, Governança e Novas Tecnologias III. VI Encontro Virtual do CONPEDI**. Santa Catarina, jun. 2023, p. 179-197.

SILVA, Cristiane Rodrigues. **História do Prontuário Médico: Evolução do Prontuário Médico Tradicional ao Prontuário Eletrônico do Paciente – PEP**. São Paulo, 2021.

A PRIVACIDADE FRENTE AO "GRANDE IRMÃO": A EFICÁCIA VERTICAL DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

Marcela Accioly Lins Magnavita[1]

RESUMO:

O presente artigo propõe-se a investigar as violações decorrentes do uso de novas tecnologias para ações de hipervigilância praticadas pelo Poder Público, de forma a desvelar a existência de um Estado de Vigilância, bem como compreender o nível de vulnerabilidade dos cidadãos frente a esse "Grande Irmão". Para tanto, utiliza-se a pesquisa bibliográfica e método hipotético-dedutivo.

Palavras chave: Proteção de Dados: Direitos Fundamentais; Estado de Vigilância.

1 INTRODUÇÃO

As atuais práticas invasivas de hipervigilância realizadas por Estados, evidenciaram uma realidade sombria que parecia ter sido deixada apenas nos contos distópicos, fazendo surgir uma fundamental necessidade de reflexão sobre como equilibrar a vigilância legítima com o direito à proteção de dados. Justifica-se a relevância do tema no aumento da hipervigilância praticada pelo poder público contra civis decorrente do uso de novas tecnologias, em diversos países, como o Brasil e outros latino-americanos que carregam heranças anti-democráticas, fazendo com que tais violações representem uma ameaça à Democracia.

Frente a isso, faz-se indispensável o resgate histórico dos Direitos Fundamentais, que nascem do anseio de proteger o indivíduo frente ao poder do

1 Graduanda em Direito pela Faculdade Baiana de Direito.

Estado, e evidenciar a eficácia vertical do Direito à Proteção de Dados. Exige-se assim, uma reflexão do Estado que queremos: De quanta privacidade estamos dispostos a abrir mão em troca de segurança? Quais informações privadas toleramos que o Estado acesse? Esse debate é essencial para o enfrentamento do Estado de Vigilância e outros desdobramentos explorados neste artigo.

2. A OPONIBILIDADE DO DIREITO À PROTEÇÃO DE DADOS AO ESTADO

O direito à proteção de dados representa um dos mais celebrados integrantes da quarta dimensão dos direitos fundamentais, pois, diante da consolidação da *data-driven economy*, informações essenciais da personalidade se tornaram verdadeiros insumos comerciais processados em escala inimaginável por meio das tecnologias de *BigData*. Para além da seara econômica, esse novo contexto possui inúmeras repercussões sociais e políticas, impactando no exercício das liberdades individuais e na própria democracia (Frazão, 2019, p. 10).

Essas repercussões derivam do fato de que a coleta dos dados possui um atributo que vai além da mera informação, possuindo o poder de incentivar e persuadir, de forma a moldar o comportamento humano, criando um novo poder chamado de "instrumentalismo" (Zuboff, 2019, p. 21-22). Assim, em razão do aumento da preocupação relacionada à coleta dos dados pessoais, foram introduzidas previsões específicas no ordenamento brasileiro, com a criação da Lei Geral de Proteção de Dados (LGPD) e a Emenda Constitucional nº 115/2022, que concedeu o seu status de direito fundamental.

No entanto, antes de ser positivado no texto constitucional, o Direito à Proteção de Dados já poderia ser extraído do Direito à Privacidade, o qual, consiste na faculdade de exigir dos outros o respeito e de se opor a violações daquilo que lhe seja próprio" (Ferraz Junior, 1993). Dentre esse "outros" inclui-se o Estado, que deve possuir limites de atuação bem definidos para garantir a devida separação das esferas pública e privada.

Nesse sentido, a LGPD, estabelece a aplicabilidade de suas disposições às pessoas jurídicas de direito público, destacando a eficácia vertical desse direito fundamental, Apesar disso, as discussões geradas pela promulgação da referida lei concentram-se sobretudo no abuso da tecnologia por parte da iniciativa privada, o chamado "Capitalismo de Vigilância"[2].

Entretanto, considerando essa circunstância que permeia a realidade social, é preciso estar atento ao fato de que, ao passo que as empresas se fortaleceram

2 Capitalismo que preve e modifica o comportamento humano para controle de mercado" (Zuboff, 2018, p. 19).

tecnologicamente, os Estados também. Desse modo, é preciso lançar os olhos ao Estado de Vigilância e a fragilidade do cidadãos frente a um Poder Público munido de tecnologias de monitoramento.

3. EVIDÊNCIAS DA EXISTÊNCIA DO ESTADO DE VIGILÂNCIA NO SÉCULO XXI

Em sua obra distópica intitulada "1984", George Orwell descreve uma sociedade futurista regida pelo medo e pela mentira, onde a palavra "privacidade" certamente foi removida do dicionário da *Novafala*. Nesse cenário, os seus cidadãos são monitorados a todo tempo pelas chamadas teletelas, que representam os olhos e ouvidos do "Grande Irmão", de forma que ninguém nunca está sozinho, como se estivessem dentro do Panóptico de Foucault.

Por essa simples descrição, é possível encontrar semelhanças desse universo distópico com o contexto atual, pois, infelizmente, "1984" e 2023 não se encontram tão distantes, uma vez que verificam-se ocorrências ao longo de todo o Globo de práticas de espionagem, monitoramento digital e hipervigilância praticadas por Governos, existindo assim um tipo de "vigilância omnipresente que anteriormente era domínio apenas dos escritores de ficção científica mais imaginativos" (GREENWALD, 2014, p. 10). Tal afirmação não tem como base apenas as experiências de Estados notadamente totalitários, mas sim a incidência dessa realidade até mesmo em países ditos como livres e democráticos, como o Brasil.

Nesses países as liberdades individuais são suprimidas por meio de um mecanismo de moeda de troca, no qual se justifica a supressão da privacidade em troca da obtenção de maior segurança. Essa busca por segurança ganha espaço como um super valor na modernidade líquida descrita por Bauman, sociedade em que vive uma aguda e crônica experiência da insegurança, resultante da convicção de que, com as capacidades adequadas e os esforços necessários, é possível obter uma segurança completa (Bauman, 2009, p. 9), fazendo com que os seus cidadãos estejam dispostos a abrir mão de qualquer outro bem jurídico em troca da sensação de segurança e proteção.

Um exemplo evidente de tal dinâmica é a promulgação em maio de 2016 de lei francesa que permitia a escuta de conversas sem a necessidade de controle judicial - bastando apenas para tanto a autorização do Primeiro-Ministro - logo após a ocorrência dos atentados contra o Charlie Hebdo (Ramonet, 2015). A justificativa para impor tais medidas de hipervigilância relaciona-se há um objetivo de defesa contra os inimigos (Chomsky, 2016), os quais inicialmente são sempre

os marginalizados e indesejados, fazendo com que se angarie apoio do restante do corpo social que ingenuamente acredita estar imune a tais práticas (Greenwald, 2014, p. 11).

Seguindo essa tendência mundial, Brasil, Chile, Colômbia, Equador, Honduras, México e Panamá compraram licenças para o uso do software de espionagem RSC[3], sendo que em três desses países foi utilizado para monitorar ativistas e opositores, evidenciando o mercado ilegal de abuso da infraestrutura de vigilância. Mesmo que esses países regulamentem a interceptação sob ordem judicial, essa disciplina legal é insuficiente em razão do potencial invasivo desse tipo de software, sendo urgente a criação de normas que estabeleçam a regulamentação da aquisição e do seu uso (Derechos Digitales, 2018, p. 420).

Ao autorizar o uso de tecnologias invasivas sob a édice de combate ao inimigo, é preciso compreender que, em verdade, o inimigo pode se tornar qualquer um de nós, pois esse tipo de política é arquitetada, muitas vezes, para proteger a autoridade estatal concentrada em poucos grupos, defendendo esses grupos contra o inimigo mais temido: toda a população (Chomsky, 2016). Isso foi evidenciado com a revelação feita por Edward Snowden ao jornalista Glenn Greenwald de que o governo Norte-Americano realizava atividades de espionagem indiscriminadamente contra cidadãos de todo o mundo.

Dessa maneira, tolerar o uso indiscriminado de tecnologias invasivas gera cenários altamente destrutivos: I - a aquisição ilegal desse tipo de software pela sociedade civil e II - o seu uso por parte do Estado contra civis sem a transparência e o devido processo legal. (Schurig, 2022), sendo eminente necessidade de discussões profundas sobre o tema.

4. PROTEÇÃO DOS CIDADÃO FRENTE AS NOVAS FORMAS DE VIGILÂNCIA

O presente contexto, evidencia que a sincera esperança de que a internet e a evolução tecnológica só poderiam representar o fortalecimento dos ideais democráticos, não se passava de uma ideia ingênua (Garay, 2023). Assim, esse cenário demanda medidas para frear o autoritarismo e o abuso das tecnologias contra a sociedade civil, a qual não se encontra protegida pela LGPD, uma vez que, apesar de incidir sob pessoa jurídicas de direito público, é inaplicável quando a coleta de dados é realizada para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º inciso III), inexistindo até o momento lei específica que regulamente tais situações. Diante disso, é urgente a atualização legislativa de norma que estabeleça

3 O RSC acessa senhas, e-mail, chamada, áudio, microfone, webcam, dados de apps e localização geográfica.

parâmetros para a aquisição e utilização de tecnologias de vigilância, bem como a transparência de seu uso.

Faz-se importante que essa atualização seja feita por meio de amplo debate com a sociedade civil, construído junto às organizações de proteção dos Direitos Humanos, associado a políticas públicas educativas que auxiliem na construção coletiva sobre os limites da vigilância e a importância da proteção de dados. Enquanto isso não é feito, cabe ampliar o espetro interpretativo do Habeas Data - remédio constitucional adequado - para sua aplicação no meio digital.

5. CONSIDERAÇÕES FINAIS

Conclui-se que o Direito à Proteção de Dados não é absoluto, sendo indispensável reconhecer que a vigilância é legítima, desde que esta seja exercida nos moldes do Estado Democrático de Direito (Ramonet, 2015). Desse modo, o que se busca é encontrar o equilíbrio entre privacidade e segurança na utilização de técnicas de vigilância, o que só será alcançado pela aplicação da ponderação cunhada por Robert Alexy, associada à reflexão inicial proposta nesse trabalho sobre o Estado que almejamos.

REFERÊNCIAS

BAUMAN, Zygmunt. **Confiança e Medo na Cidade.** 1 ed. Rio de Janeiro. Editora Zahar, 2009. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7629446/mod_resource/content/1/Confianca%20e%20Medo%20na%20Cidade%20-%20Zygmunt%20Bauman.pdf Acesso em: 31 ago 2023

CHOMSKY, Noam. **O Estado de Vigilância nos países livres.** In Instituto Humanitas UNISINOS. 27 set 2016. Disponível em: https://www.ihu.unisinos.br/categorias/185-noticias-2016/560481-o-estado-de-vigilancia-nos- paises-livres-artigo-de-noam-chomsky. Acesso em: 05 ago 2023.

DERECHOS DIGITALES. **Hacking Team na América Latina.** In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas. **Tecnopolíticas da vigilância: perspectivas da margem** . 1. ed. São Paulo. Boitempo, 2018, p. 417 - 422. Disponível

em: https://medialabufrj.net/wp-content/uploads/2020/10/Tecnopoliticas-da-vigilancia_miolo_do wnload.pdf Acesso em: 31 ago 2023

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados.** In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. - São Paulo : Thomson Reuters Brasil, 2019, p. 11 - 18.

FERRAZ JR., Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política.** São Paulo: RT, nº 01, 1993, p. 439-459

GARAY, Vladmir. **Derechos Digitales en America Latina: por tecnolgoias al servicio del bein comun y el desarrolo integral de la sociedad.** In Derechos Digitales. 11 ago 2023. https://www.derechosdigitales.org/22185/derechos-digitales-en-america-latina-por-tecnologias-al-servicio-del-bien-comun-y-el-desarrollo-integral-de-la-sociedad/ Acesso em: 31 ago 2023

GREENWALD, Glenn. **No Place to Hide: Edward Snowden, the NSA and the Surveillance State.** Penguin Group. London, 2014.

RAMONET, Ignacio. **Em troca de suposta segurança, sociedade admite estado de vigilância maciço.** In Instituto Humanitas UNISINOS. 01 dez 2015. Disponível em: Acesso em: https://www.ihu.unisinos.br/78-noticias/549637-ignacio-ramonet-em-troca-de-suposta-seguranca-sociedade-admite-estado-de-vigilancia-macico Acesso em: 11 ago 2023.

SCHURIG, Sofia. **O Distópico Estado de Vigilância no Brasil.** In Jacobin Brasil. 2022. Disponível em: https://jacobin.com.br/2022/01/o-distopico-estado-de-vigilancia-no-brasil/. Acesso em: 31 ago 2023.

A DISCRIMINAÇÃO ALGORÍTMICA E O DIREITO SOCIAL AO TRABALHO SOB UMA PERSPECTIVA DE GÊNERO

Ana Beatriz de Souza Soares[1]

INTRODUÇÃO

No dia 08 de março comemora-se o dia das mulheres, em lembrança às trabalhadoras das fábricas que outrora lutaram por melhores condições de trabalho. O mundo contemporâneo traz à tona novos desafios, voltados com a questão dos dados. Há uma forma de opressão contemporânea que imputa o machismo aos algoritmos quando estes vão definir os rumos do futuro profissional das pessoas, e dados pessoais que não teriam pertinência no ambiente profissional podem acabar sendo usados contra as mulheres. O mundo digital acelera as discriminações, é mais fácil ter acesso a uma infinidade de dados pessoais. O presente *paper* irá tratar da discriminação algorítmica de gênero nas seleções laborais, salientando que o direito social ao trabalho e o direito à proteção de dados estão positivados na Constituição Federal.

1. A DISCRIMINAÇÃO ALGORÍTMICA EM PROCESSOS DE SELEÇÃO E AS PAUTAS DAS MULHERES EM MEIO AO DEBATE

Com as inúmeras demandas da contemporaneidade, e aproveitando os avanços nas tecnologias, encontrou-se a dita solução de usar o algoritmo para processos de recrutamento e seleção, como alternativa supostamente eficiente e eficaz para medir a qualidade técnica dos profissionais, estipular parâmetros e decidir quem merecia avançar na seleção ou ser diretamente contratado repercutiu

1 Graduanda em Direito pela Faculdade Baiana de Direito. E-mail: abdssoares@outlook.com

da Amazon, demonstram como o processo de machine learning repete os erros dos seres humanos, reforçando padrões discriminatórios, repetindo e perpetuando padrões antigos. O que temos aqui é uma tecnologia sem transparência e sem explicabilidade, que não traz confiança ou resultados fidedignos, o algoritmo apenas acaba exacerbando as discriminações latentes na contemporaneidade. Inegavelmente, há graves erros de governança algorítmica, e as mulheres estão mais vulneráveis neste processo.

Vale ressaltar que os algoritmos estão sendo usados para definir um direito social das mulheres, o direito ao trabalho, que é um fator extremamente relevante para sua subsistência e para a manutenção de sua família, ou seja, um erro algoritmo seria extremamente prejudicial para a vida do indivíduo. A priori, seria uma inofensiva forma de agilizar processos de RH, mas na prática, há riscos de grandes injustiças. Nos processos de seleção do gênero, há uma clara vantagem no padrão de profissionais homens e brancos, e um disprivilégio às mulheres. Se optar-se por adentrar nos recortes dentro do gênero feminino, o debate é ainda mais delicado, por prejudicar demasiadamente mulheres negras, mulheres mães, mulheres trans, exemplificativamente. Portanto, é inadmissível aceitar esse tipo de injustiça de um algoritmo que foi proposto para julgar o futuro profissional das pessoas.

O algoritmo da Amazon analisava currículos dando notas de 1 a 5 estrelas, e a simples menção ao termo "mulher", já penalizava a candidata pois a tecnologia entendia que nos últimos anos, a maioria dos funcionários eram homens, portanto, devia-se repetir o padrão para garantir boa qualidade de contratação. Diz-se que houve erro no treinamento da tecnologia.

Nota-se ausência de transparência nos processos e fica um forte impacto negativo do algoritmo da vida de muitos (as). Nota-se que o direito social fundamental de acesso ao trabalho é afrontado, por meio de uma decisão algoritma repleta de discriminação e não isonômica. Fere- se, também, o princípio da explicabilidade. Urge analisar os casos à luz do Direito e das legislações existentes pertinentes. É preciso esclarecer que a inteligência artificial é sim um mecanismo para facilitar processos e auxiliar a sociedade, no entanto, há uma barreira que não pode ser ultrapassada para o uso das IAs: os direitos humanos. Os direitos básicos e que estão no cerne da necessidade dos homens não podendo, em hipótese alguma, ser negligenciados por causa de um algoritmo.

No Brasil, ainda há pouca maturidade na legislação sobre o tema, mas é possível citar países mais avançados no assunto, como Portugal, que criou a "Carta de Direitos Humanos na Era Digital". O documento determina que:

> *Artigo 9.o Uso da inteligência artificial e de robôs 1 — A utilização da inteligência artificial deve ser orientada pelo respeito dos* ***direitos fundamentais****, garantindo um justo equilíbrio entre os*

> *princípios da explicabilidade, da segurança, da transparência e da responsabilidade, que atenda às circunstâncias de cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação.*

No que tange à não discriminação, fica evidente o desrespeito do algoritmo. Mulheres que são mães, por exemplo, são prejudicadas em detrimento daquelas que não geraram. Mulheres negras são desprivilegiadas em face de mulheres brancas, e daí por diante. Certos dados pessoais, muitas vezes configurados como dados sensíveis, são usados para desqualificar as candidatas, apesar de não corresponderem ao seu desempenho ou à sua competência.

Destrinchando o que temos na legislação brasileira, pode-se fazer um paralelo com o Art. 6o da Lei Geral de Proteção de Dados Pessoais (LGPD):

> *Art. 6o As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*

Por todo o exposto, o tratamento é notoriamente discriminatório. Aproveitando a temática trazida na LGPD, cabe complementar que o algoritmo violaria o que é dito no caput do art. 5o da Constituição Federal, que diz que todos os cidadãos são iguais em face à lei, não devendo existir distinções de qualquer natureza.

No caso em questão, cabe fomentar um discurso sobre direitos difusos coletivos. Afinal, o procedimento prejudica inúmeras pessoas, não sendo uma situação privada, mas sim uma situação coletiva. O capitalismo de dados aqui é o responsável por reduzir indivíduos a combinações algorítmicas, sem revisões ou um procedimento seguro, afetando um direito social: o direito ao trabalho. É dever do Estado proporcionar meios de acesso ao trabalho e emprego digno, segundo legislações brasileiras, e a ANPD deve realizar auditoria dos casos.

Não obstante, seguindo na análise das legislações brasileiras, fere-se o direito à informação e à transparência.

> *Art. 6o As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*

Na Lei Geral de Proteção de Dados, o princípio da transparência traz a urgência em garantir informações claras para os titulares de dados sobre os

tratamentos realizados. Neste caso, a transparência é completamente negligenciada e é inviável usar o discurso de "segredo comercial e industrial", por estarmos falando de um tratamento de dados com fins de garantir um direito extremamente relevante.

Nesse âmbito, cabe citar a importância do instituto de um relatório de impacto, que deveria ser publicado previamente a todo e qualquer processo de seleção com algoritmos, para trazer à tona medidas de mitigação de riscos, benefícios x malefícios, explicações e transparência. Aqui, a explicabilidade deveria descomplicar os processos para a população e evidenciar a forma de funcionamento do algoritmo. Ainda, um debate pertinente gira em torno das revisões de decisões automatizadas. No Artigo 20 da LGPD, legislação brasileira, é dito que:

> *Art. 20. O titular dos dados tem direito a solicitar a* ***revisão de decisões*** *tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.*

Neste caso, o direito à revisão da decisão seria simplório demais. O eventual dano instaurado é quase irreversível, já que a mulher pode ter perdido meses de um salário em um cargo que poderia ser seu eventualmente. Pela seriedade do tema, falta a mitigação de riscos, tendo em vista que mecanismos tardios são insuficientes quando já há um risco fixado. Aplicando a ponderação entre os direitos das mulheres ao emprego e a (in)eficácia do método de seleção em questão, percebe-se um prejuízo desproporcional na vida destas.

CONCLUSÕES E CONSIDERAÇÕES FINAIS

Urge esclarecer que deve-se analisar as legislações pertinentes, nacionais e internacionais, e seus princípios e fundamentos, analisando os casos de seleção com IA com uma visão pluralista e sistêmica, capaz de analisar a teoria dos Direitos Fundamentais. Deve- se ponderar os prós e os contras no uso de determinado algoritmo, garantindo a elaboração de relatórios de impacto. As problemáticas não são objetivas, deve-se prezar pela proporcionalidade e pela compatibilidade das resoluções de conflitos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 de setembro de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 01 de setembro de 2023.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados comentada.** 3. ed. São Paulo: Revista dos Tribunais, 2021.

SAN FRANCISCO. **Amazon scraps secret AI recruiting tool that showed bias against women.** DASTIN, Jeffrey. OCTOBER 10, 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 01 de setembro de 2023.

FALTA DE INTEROPERABILIDADE ENTRE DISPOSITIVOS IOT: DESAFIOS PARA A PROTEÇÃO DE DADOS PESSOAIS

Eliseu Almeida Brandão da Silva

INTRODUÇÃO

No cenário atual de contínuo avanço da tecnologia, a sociedade está cada vez mais entrelaçada e interdependente da Internet. Nos últimos anos, houve um aumento expressivo no número de objetos físicos interconectados na rede, que deram origem ao conceito de Internet das Coisas (IoT).

Dispositivos IoT têm o potencial de transformar a maneira como interagimos com o mundo físico e estão presentes em uma ampla gama de setores, incluindo o residencial. Entretanto, a proliferação de "casas inteligentes", compostas por uma variedade de dispositivos conectados à Internet, como lâmpadas inteligentes, assistentes virtuais, câmeras de segurança, carros, fechaduras e robôs de limpeza, levanta questões críticas de segurança e privacidade de dados.

Em muitos casos, esses produtos são incompatíveis entre si, o que resulta em uma complexidade de agentes de tratamento de dados, protocolos de comunicação, formatos de dados e métodos de segurança. Assim, a introdução de dispositivos IoT nas residências levou à coleta de uma quantidade massiva de dados pessoais de várias fontes, o que representa desafios significativos no controle e na proteção desses dados. Este artigo discute os desafios para garantir a segurança de dados pessoais diante da falta de interoperabilidade entre dispositivos IoT.

CONCEITO DE INTEROPERABILIDADE

Interoperabilidade é a capacidade de sistemas e organizações trabalharem em conjunto de forma eficaz e eficiente, o que permite a integração de diferentes

dispositivos e fabricantes. Ela é um requisito importante na proteção de dados pessoais, uma vez que permite o suporte transfronteiriço de políticas de privacidade entre diferentes tecnologias, padrões e legislações (Porambage, et al., 2016, p. 7).

Essa necessidade se verifica pelo fato de que se os dados pessoais estão armazenados em sistemas que não se comunicam entre si, os agentes de tratamento podem ter dificuldade para acessar, verificar, atualizar ou corrigir os dados. Podem existir padrões ou formatos diferentes que dificultariam extrair, analisar ou interpretar os dados, bem como diferentes normas e regulamentos os quais os dados estão sujeitos que poderiam gerar dificuldades na conformidade legal dos dados, ou uma fragmentação e dispersão dos dados que culminariam em dificuldades para monitorar ou avaliar o tratamento. Esses problemas podem facilitar violações de dados, dificultar atualizações de segurança e tornar mais difícil para os titulares de dados acessar, retificar, portar ou excluir seus dados pessoais.

PROBLEMAS DA FALTA DE INTEROPERABILIDADE EM DISPOSITIVOS IOT

Dessa maneira, a falta de interoperabilidade entre dispositivos IoT é um desafio significativo para a proteção de dados pessoais coletados em residências, que geralmente incluem informações sensíveis relacionadas à segurança, saúde, biometria e rotina dos indivíduos. Em maio deste ano de 2023, a influenciadora digital americana Kurin Adele relatou um inconveniente que envolvia proteção de dados através da plataforma de vídeos TikTok, contando com milhões de visualizações e relatos parecidos nos comentários do vídeo (Pazero, 2023). Na sua dicção, pessoas desconhecidas invadiram sua babá eletrônica e se passaram por ela e pelo pai do seu filho, sem que ela soubesse por quanto tempo os invasores se comunicaram com a criança. Esse tipo de incidente não está limitado ao exterior, pois, no Brasil, a Polícia Federal registrou 141 invasões em câmeras IP em 35 municípios em 2020 (Globo, 2020).

Esses exemplos demonstram como a falta de interoperabilidade entre dispositivos IoT pode facilitar as violações de dados pessoais de duas maneiras. Primeiro, ela pode permitir que os invasores acessem diretamente os dispositivos, sem necessidade de quebrar a segurança. Foi o que aconteceu no caso da influenciadora americana, que teve sua babá eletrônica invadida por hackers que acessaram o dispositivo diretamente da Internet. Segundo, a falta de interoperabilidade pode dificultar a atualização de segurança dos dispositivos. Isso foi o que aconteceu no caso das câmeras IP invadidas no Brasil, que foram exploradas por hackers por meio de vulnerabilidades que não foram corrigidas devido à falta de interoperabilidade.

Logo, os problemas de segurança suscitados pelos aparelhos IoT podem ser agravados quando não aderem a um ecossistema que garanta um padrão

de segurança de dados, implementando medidas adequadas de proteção, porque assim eles correm um maior risco de apresentar vulnerabilidades. Dessa maneira, a falta de padronização de segurança constitui um grave empecilho na salvaguarda da privacidade de dados, uma vez que não há garantia de um nível adequado de proteção para todos os produtos IoT que são adquiridos em casa por parte do consumidor.

Além disso, quando dispositivos não são compatíveis com atualizações ou correções de vulnerabilidades, é mais fácil que sejam descobertas novas brechas que não serão futuramente corrigidas. Nesse caso, o monitoramento da segurança também pode ser debilitado pela diversidade de fabricantes, o que resulta na falta de visibilidade das possíveis ameaças e riscos que poderiam ser corrigidos.

Na maioria dos casos, o consumidor não tem noção dos riscos que corre ao adotar aparelhos do tipo em casa. Ele pode ser vítima de vazamento de dados, interceptações ou intromissões de terceiros a qualquer instante, sem saber se ocorreram, quando ocorreram ou por quanto tempo ocorreram. Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) prevê no seu artigo 6º que as atividades de tratamento de dados pessoais devem observar o princípio da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. No entanto, a falta de interoperabilidade pode dificultar o cumprimento desse requisito, dado que os agentes de tratamento podem não ser capazes de implementar medidas de segurança que sejam compatíveis com todos os dispositivos IoT envolvidos no processo de tratamento.

Em outra perspectiva, a falta de interoperabilidade pode levar a lacunas de segurança, uma vez que um dispositivo vulnerável pode afetar todos os outros. Um exemplo disso é um modem que, se não for configurado com o mesmo padrão de segurança dos demais aparelhos, pode ser invadido com maior facilidade, o que afetaria toda a rede wi-fi e os aparelhos nela conectados.

A falta de interoperabilidade entre os dispositivos IoT ainda pode dificultar a implementação de medidas de segurança e o exercício dos direitos dos titulares de dados. Quando diferentes fabricantes utilizam tecnologias que são incompatíveis entre si, os dispositivos IoT podem operar de maneira independente, sem compartilhar informações. Esses sistemas fechados acabam dificultando a implementação de medidas de segurança, já que os dados pessoais ficam isolados em "ilhas".

Além disso, essa fragmentação exige que o usuário gerencie e monitore múltiplas plataformas e políticas de privacidade separadamente. Nesse sentido, aduz Bioni (2019) que a adoção de padrões técnicos para a interoperabilidade de dispositivos conectados, através de uma linguagem comum, pode abrir a possibilidade para que os seus usuários emitam comandos comuns em torno das suas preferências de privacidade.

Dessa forma, quando não há padrões de interoperabilidade, é mais difícil para os titulares de dados acessar, retificar, portar ou excluir seus dados pessoais, pois eles podem precisar usar diferentes ferramentas e processos para acessar dados de diferentes dispositivos. Ademais, quando os dispositivos IoT não são interoperáveis, pode ser mais difícil para as autoridades investigar violações de dados, uma vez que podem precisar acessar dados de diferentes dispositivos para compreender a extensão da violação.

CONCLUSÃO

A Internet das Coisas é um conceito promissor que ganha cada vez mais repercussão no cenário global. Já são comuns hoje em dia as chamadas casas inteligentes, que abarcam inúmeras dessas tecnologias para as mais diversas finalidades. Entretanto, esse progresso é acompanhado por riscos silenciosos no que diz respeito à proteção de dados pessoais. A falta de interoperabilidade entre os dispositivos é um dos principais elementos que dificultam a introdução segura desses aparelhos nas residências, pois geram risco de dados desprotegidos em sistemas isolados, sem garantia de padrões adequados de segurança, e a dificuldade de tutela diante de violações aos direitos do titular de dados.

Para mitigar esse desafio, é importante que os fabricantes de dispositivos IoT adotem padrões de interoperabilidade abertos e cooperem entre si para desenvolver soluções com o intuito de que os ecossistemas se comuniquem e compartilhem dados entre si de maneira mais eficiente. Os usuários também podem tomar medidas para proteger seus dados pessoais, mesmo quando os dispositivos não são interoperáveis, como utilizar aqueles com recursos de privacidade integrados, como criptografia de dados e controle de acesso.

Para um aprofundamento do tema da pesquisa, será necessário explorar como a falta de interoperabilidade entre dispositivos IoT pode dificultar a aplicação da legislação, afetar os direitos do titular de dados, dificultar a implementação de medidas de segurança e investigações de violações de dados. Além disso, será necessário identificar os padrões de interoperabilidade atualmente observados, bem como aqueles que são mais compatíveis com a legislação, e avaliar as oportunidades de melhoria existentes. Para isso, serão necessários estudos sobre padrões e tecnologias de interoperabilidade, análises de impactos regulatórios e estudos de casos envolvendo dispositivos IoT.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Gen, Editora Forense, 2019.

G1. **Veja cuidados para evitar que câmeras e babás eletrônicas sejam invadidos.** 10 abr. 2023. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/04/10/veja-cui dados-para-evitar-que-cameras-e-babas-eletronicas-sejam-invadidos.ghtml. Acesso em: 14/09/2023.

PAZERO, Letícia. **Americana afirma que teve babá eletrônica hackeada: "Falavam com meu filho".** CNN Brasil, São Paulo, 10 mai. 2023. Disponível em: https://www.cnnbrasil.com.br/entretenimento/americana-afirma-que-teve-baba-eletronica-hackeada-falavam-com-meu-filho/. Acesso em: 14/09/2023.

PORAMBAGE, Pawani et al. **The quest for privacy in the internet of things.** IEEE Cloud Computing, v. 3, n. 2, p. 36-45, 2016.

AUTOMÓVEIS: UM PESADELO À SUA PRIVACIDADE?

Evelyn Pastorello

Os avanços tecnológicos estão fazendo com que cada vez mais os indivíduos fiquem à mercê das mais variadas empresas dos mais diversos ramos, uma vez que seus dados pessoais passam a ocupar um importante papel: ser moeda de troca. Nesse ínterim, a proteção dos dados pessoais é um assunto que deve ser discutido e pensado pela sociedade de forma corriqueira, na medida em que as empresas se encontram em uma corrida de "quem" coleta mais informações pessoais, criando mecanismos impensáveis pelos cidadãos para assim o fazer, visando apenas o lucro que terá com isso. Deste modo, é possível notar que a privacidade se tornou algo almejado e só possível nos sonhos, pois na realidade o que se tem é uma coleta de dados pessoais que ocorre de maneira exacerbada realizada por tudo e por todos. É a ideia de que não é viável fazer mais nada se o sujeito não abrir mão de seus segredos que, em tese, só deveria lhe pertencer.

É indubitável a enorme coleta de dados pessoais que se tem atualmente, porém é inacreditável quais dados são coletados, quem os coletam e o que fazem com eles. Sob esse prisma, importante questão a se discutir é os carros modernos, visto que a pessoa quando compra um automóvel almeja sua liberdade de ir e vir, sua liberdade de ficar sozinha no interior do carro em segurança, sem ninguém importunando, ouvindo sua playlist favorita ou eventualmente conversando com alguém por ligação enquanto realiza o seu trajeto. Com isso, muitos conectam seus smartphones aos veículos para poder ter essa acessibilidade de forma mais fácil e prática. Sendo assim, chega a ser perturbador e até mesmo assustador o fato de que o momento de provável despreocupação do motorista que ali se encontra, precisa ser o momento de mais preocupação com os rastreadores, as câmaras, os sensores, os microfones que captam cada movimento que é realizado e cada palavra que é falada, tornando os carros modernos em verdadeiras ameaças à privacidade.

A lei n° 13.709/08 (Lei Geral de Proteção de Dados Pessoais), conhecida como LGPD, foi uma grande conquista no âmbito da proteção de dados, no entanto não

se pode ignorar a realidade. Dessa forma, no momento em que se observa marcas de automóveis coletando, de modo ilícito, mais dados pessoais que o necessário - violando o princípio da necessidade, previsto no art. 6°, III, da lei supracitada - e utilizando-os por um motivo diferente de operar o veículo e gerenciar o relacionamento com o comprador, fica claro o poder que os fabricantes de automóveis têm nas mãos. Em contrapartida, só é possível ter conhecimento sobre a atuação das empresas em relação aos dados de caráter pessoal por causa da existência de leis - como é o caso da LGPD quando aborda em seu art. 6°, IV e VI, os princípios de livre acesso de transparência - que tornam ilegal o ato de não divulgar essas informações, o que demonstra a importância da normatização sobre esse assunto.

Desde algum tempo que os carros se encontram em um processo de evolução, é só ver que na década de 1970 eles já tinham algum tipo de computador. O que é novo é o número e a quantidade de coisas que eles controlam. Logo, o tempo passa e mais recursos dos carros são alimentados por sistemas de computadores que também se conectam à internet, e isso não é um fato que alcança apenas os carros futuristas de última geração, mas também os "veículos básicos". Sob essa perspectiva, a consultoria McKinsey prevê que até 2030, 95% dos novos veículos vendidos globalmente serão conectados – uma realidade que já está presente a cada dia que passa.

Os carros que já detém recursos e comandos mais avançados que dispensaram os botões, apresentando sensores sensíveis ao toque e telas que funcionam com um simples toque do dedo ou até mesmo com um pedido verbal, são um fator que deve levantar sérias preocupações, uma vez que são muitas as informações "privilegiadas" que as empresas automobilísticas conseguem ter acesso. São exemplos: informações médicas, genéticas, quão rápido aquele sujeito dirige, onde ele dirige, quais músicas ele costuma ouvir no carro, etc. Isso acaba sendo de muita utilidade para que a própria montadora consiga produzir seu marketing, mas, para além disso, ela pode compartilhar os dados pessoais coletados com prestadores de serviços, corretores de dados ou outras empresas sobre as quais não se tem muitas informações, ou, diante de um "pedido informal", com o governo ou com as autoridades policiais. Ademais, algumas marcas de automóveis - Ford, Audi e Toyota - ainda vendem essas informações privadas. Mudando seu foco de vender carros para vender dados, o que demonstra o risco que os consumidores estão submetidos. (Jen Caltrider, 2023)

A grande relevância dessa questão é que, ao contrário dos aplicativos ou dispositivos domésticos inteligentes - Alexa, Amazon, Google -, a maioria dos motoristas não estão nem cientes de que esses fabricantes conseguem ter acesso a tantas informações de suas vidas - desde a crença filosófica até gravações de voz -, ficando ainda mais distantes de ter o poder de desativá-los. Para mais, mesmo aqueles que têm acesso a política de privacidade de empresas como Honda, BMW, Mercedes-Benz e Toyota, observam o uso de uma linguagem vaga, usada estrategicamente para deixar a porta aberta para que seja possível a coleta de mais dados, indo além daqueles que estão especificados em suas políticas, tornando impossível que o

indivíduo consiga saber de fato quais são todas as informações de sua vida que estão sendo coletadas e armazenadas. (Olhar Digital, 2023)

Para além do exposto, ainda há mais uma questão a ser analisada, a falta de responsabilidade e compromisso das empresas automobilísticas no papel de controladora que se colocam. "Controlador" é conceituado na LGPD em seu art. 5°, VI, como pessoa a quem compete as decisões referentes ao tratamento de dados pessoais, em contrapartida o inciso VII traz a figura do operador - pessoa que realiza o tratamento de dados pessoais em nome do controlador. Dessa maneira, por ser o controlador que contrata o operador, ele deve tomar as devidas precauções com relação a proteção dos dados e será responsabilizado por eventuais falhas do operador. Em decorrência disso, o controlador deve fiscalizar e instruir corretamente as ações dos operadores. No setor automotivo, observa-se que as diretrizes de segurança que deveriam ser adotadas pelas marcas ficam só no "deveriam", no cenário ideal, posto que muitos são os casos em que há vazamentos de dados dos motoristas. Por exemplo, a Volkswagen e sua subsidiária Audi que sofreram uma violação de dados que afetou 3,3 milhões de usuários; a Toyota que vazou dados de 2,15 milhões de usuários ao longo de 10 anos, entre 2013 e 2023; e a Mercedes-Benz que, em junho de 2022, divulgou uma falha de dados por parte de um fornecedor terceirizado que expôs as informações pessoais - incluindo nomes, endereços residenciais, endereços de e-mail e números de telefone - de até 1,6 milhão de clientes em potencial e clientes reais. (Jen Caltrider, 2023)

Um relatório divulgado pela Mozilla Foundation, uma organização sem fins lucrativos, revelou que os carros possuem as piores políticas de privacidade quando comparados com outras categorias de produtos e faz um alerta, na medida que a menos que não se trate de um Chevrolet de 1967, o sujeito pode estar em "risco". Outrossim, das 25 marcas de veículos analisadas pela Mozilla, dentre elas Audi, Toyota, Tesla e Ford, nenhuma atendeu aos padrões básicos de privacidade, tendo ainda a Nissan admitido que seus veículos coletam dados sobre a vida sexual dos motoristas, mas, previsivelmente, não explicou quais dados são coletados ou como são obtidos. (Jen Caltrider, 2023)

Destarte, é notório que muito ainda se tem a pesquisar sobre esse assunto tão nebuloso e desconhecido por grande parte da população que, por sua vez, quando vai comprar o carro a última coisa que pensa é o quanto ele pode espionar a sua vida.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei n° 13.709**, de 14 de agosto de 2018. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Diário Oficial da União, Brasília, DF,

15/08/2018. Seção I, página 59.

CALTRIDER, Jen. et al. *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*. Fundação Mozilla, 2023. Disponível em: https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/?utm_source=the%20news&utm_medium=newsletter&utm_campaign=08_09. Acesso em: 08 de setembro de 2023.

OLHAR DIGITAL. **Seu Direito Digital: seu carro pode estar coletando seus dados!**. YouTube, 08 de setembro de 2023. Disponível em: https://youtu.be/L121kINHDoA?si=0gH-wQvDmmLRA5tz. Acesso em: 09 de setembro de 2023.

THE NEWS. **Seu carro te rastreia mais que seu Apple Watch**. Disponível em: thenewscc.com.br. Acesso em: 08 de setembro de 2023

DESAFIOS ÉTICOS E LEGAIS DO USO DE DADOS BIOMÉTRICOS NO TRANSPORTE PÚBLICO: O CASO DO METRÔ DE SÃO PAULO

Giulia De-gino D'Antonio[1]

1 INTRODUÇÃO

Em que pese a crescente adoção de modelos de negócios em *big data* envolvendo algoritmos de Inteligência Artificial (IA) e Internet das Coisas (*Internet of Things - IoT*) represente um notório avanço tecnológico, a ação civil pública proposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) em face da empresa Concessionária Da Linha 4 Do Metrô De São Paulo S.A. (Via Quatro), decorrente da coleta e tratamento de imagens e dados biométricos, isto é, dados pessoais sensíveis, sem a devida anuência das pessoas que passavam pelas sete estações que formam a linha Amarela levanta importantes questionamentos sobre privacidade, proteção de dados pessoais e os seus limites.

Em que pese o papel dos dados biométricos no melhoramento de publicidades e propagandas, através da identificação quase instantânea das reações, cabe questionar: como conciliar o uso de dados biométricos com os princípios legais e éticos do ordenamento jurídico, a fim de garantir o crescimento econômico e o avanço da tecnologia sem comprometer a privacidade e os direitos individuais dos cidadãos? A problemática em questão possui uma pertinência extremamente relevante do ponto de vista sociojurídico vez que se trata de uma temática extremamente atual, afinal, o Direito está se habituando à forma com que regula determinadas condutas que tangenciam os dados pessoais e o digital.

No que tange ao procedimento técnico de pesquisa, o presente trabalho se caracteriza como predominantemente bibliográfico. Quanto ao método de pesquisa, a dedução será utilizada visando analisar a veracidade das hipóteses formuladas com base nas premissas jurídicas da doutrina e da legislação no

1 Graduanda em Direito pela Faculdade Baiana de Direito. E-mail:contato@giuliadantonio.com

decorrer do artigo. Amparado na metodologia de Popper serão levantados questionamentos acerca dos desafios éticos e legais do uso de dados biométricos, os quais buscarão ser respondidos pelo falseamento.

Este estudo busca explorar os desafios da coleta, armazenamento e tratamento de dados biométricos coletados para publicidades em transportes públicos. As implicações éticas e jurídicas decorrentes dessa prática fomentam o debate a respeito do equilíbrio entre inovação tecnológica e o respeito aos direitos fundamentais dos cidadãos, plenamente assegurados pela Constituição Federal e pela Lei Geral de Proteção de Dados.

2 DADOS BIOMÉTRICOS E O ORDENAMENTO JURÍDICO BRASILEIRO

A priori, cumpre destacar que dados biométricos, à luz da Lei nº 13.709/18, art. 5º, inciso II são, inequivocamente, dados sensíveis. Viviane Maldonado e Renato Blum explicam que esses dados pessoais são chamados de "sensíveis" porque podem gerar algum tipo de discriminação, além de implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares, principalmente quando se trata de dados biométricos, dada a sua natureza mais crítica (Maldonado; Blum, 2019, p. 69-70).

A Constituição Federal, por sua vez, esculpe em seu art. 5º, inciso X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas como direitos fundamentais (BRASIL, 1988). A disposição constitucional não só faz cristalizar a necessidade e, principalmente, a importância de proteger a esfera pessoal dos cidadãos através da custódia dos seus dados pessoais, sejam eles sensíveis ou não, como também impõe limites ao tratamento desses dados por parte de entidades públicas e privadas.

Ressalta-se, no entanto, que apesar da motivação da conceituação dessa categoria especial de dados pessoais ser fruto de uma observação pragmática da diferença que apresenta o efeito do tratamento desses dados em relação aos demais (Doneda, 2006, p.161), a maior proteção concedida, principalmente a respeito de dados biométricos, não é sinônimo de impossibilidade de tratamento.

Apesar do consentimento inequívoco e da finalidade específica no tratamento de dados sensíveis serem princípios cruciais a serem observados, o art. 11º da LGPD traz em seus incisos oito hipóteses que facultam o seu tratamento, as quais vão além do consentimento, sem deixar de garantir que a coleta e o processamento de informações biométricas sejam realizados de maneira ética e legal.

Nesse ponto, diante da (des)necessidade de consentimento para a coleta de dados biométricos, surge o questionamento: qual seria o fator capaz de impedir a instalação do sistema Portas Interativas Digitais no Caso do Metrô de São Paulo, responsável por captar as emoções dos usuários da Linha Amarela e, ao mesmo tempo, facultar o uso de equipamentos de reconhecimento facial no Carnaval de Salvador?

3 CARNAVAL DE SALVADOR X METRÔ DE SÃO PAULO

A resposta, nada simples, pode ser explicada por uma série de fatores, incluindo questões legais, éticas e de finalidade, que, no caso do Carnaval de Salvador, versava sobre uma questão de segurança pública[2] e de necessidade de controle de acesso a um eventos de grande aglomeração, subsumindo-se às alíneas b) e e) do art. 11º, inciso II da LGPD[3].

A finalidade evoca também a transparência acerca da maneira em que os dados serão tratados, desde a coleta até o seu armazenamento. No Carnaval de Salvador, a finalidade é quase intuitiva: garantir a segurança do evento. No caso das portas interativas no Metrô de São Paulo, a finalidade de capturar emoções para fins publicitários pode ser vista como menos clara, mais invasiva e abusiva, afinal, o objetivo é a maximização de lucros privados.

Um último ponto de divergência seria a expectativa razoável de privacidade esperada pelas pessoas, isto é, enquanto o Carnaval de Salvador é a festa de rua mais famosa do muito, estações de metrô são espaços de transporte público e, por isso, instalar portas interativas digitais que, segundo a própria Ré declarou no processo, é capaz de contar pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, horas de pico de visualizações, captação de expressões e emoções sem o conhecimento ou consentimento desses usuários pode ser vista como uma violação dessa expectativa.

Contudo, é sabido que a mera quebra de expectativa não foi o fator causador da condenação da Requerida ao pagamento de indenização por danos morais coletivos no valor de R$100.000,00 (cem mil reais), mas sim o fato de

2 Segundo o Governo da Bahia, as lesões corporais apresentaram queda de 56%.Os roubos e furtos também recuaram, de 1.153 para 898 casos. No acumulado, ações das polícias Militar e Civil prenderam em flagrantes 25 criminosos. No total, somando com os 49 foragidos localizados pelo Reconhecimento Facial, 74 pessoas envolvidas com crimes foram retiradas dos circuitos do Carnaval de Salvador.

3 Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; e) proteção da vida ou da incolumidade física do titular ou de terceiro;

que o tipo de coleta/tratamento realizado sem consentimento dos usuários não incidia em nenhuma das hipóteses da Lei nº 13.709/18.

4 OS DESAFIOS ÉTICOS ENVOLVIDOS

Ante a improcedência suscitada pela empresa concessionária no sentido de que as portas digitais "não captavam imagem definidas atribuídas a pessoas identificadas, mas apenas detecta rostos e expressões", surgem alguns desafios éticos que demandam análise no contexto jurídico. Não se encaixando nas hipóteses do inciso II do art. 11º, em razão da privacidade e da autonomia individuais é imprescindível que os titulares dos dados pessoais estejam devidamente cientes de que suas emoções estão sendo monitoradas e registradas.

Apesar de não terem provado o que alegam, tomando como se verdadeiros fossem os fatos narrados, a ausência de transparência nesse processo de coleta de dados, por si só, suscitaria questionamentos quanto à legalidade e à ética subjacentes, afinal, é inegável o objetivo de melhoria das publicidades como forma de maximização dos lucros.

Nas palavras de Stefano Rodotá, o cidadão não pode ser visto como simples fornecedor de dados, ele tem que ter poder de controle sobre esses dados, para se estabelecer o equilíbrio na concentração de poder (2008, p. 36). Ressalta-se ainda que os mais diversos perfis passam pelos transportes públicos todos os dias, fazendo com que a questão ética se mostre ainda mais sensível quando diante da vulnerabilidade de grupos como crianças ou pessoas com problemas emocionais, trazendo à tona outras questões dignas de estudo.

5 CONSIDERAÇÕES FINAIS

Diante da análise do Caso do Metrô de São Paulo e das suas portas inteligentes, apesar do inegável papel dos dados biométricos no avanço da tecnologia e na segurança pública, inúmeras são as questões - majoritariamente éticas - postas à prova, sendo um ponto crítico que merece a atenção do Judiciário.

A coleta em massa feita por empresas privadas através da captação das mais diferentes expressões faciais, não só sem consentimento mas visando o lucro através da reação às publicidades exibidas emergem preocupações absolutamente legítimas sobre a eficácia das normas jurídicas que asseguram a privacidade e a

proteção de dados pessoais, o que é um direito fundamental reconhecido pelo ordenamento jurídico brasileiro.

Apesar da base sólida oferecida pelo ordenamento jurídico, o caso em tela ratifica como abordagem cuidadosa e atualizada do magistrado diante das inovações tecnológicas é crucial para o bem estar do coletivo e, não por outro motivo, os direitos individuais, como a privacidade e responsabilidade coletiva, são pilares essenciais que devem ser observados para garantir uma abordagem ética e legalmente sólida nesse contexto.

REFERÊNCIAS

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006. p. 161.

DUARTE, T. Júlia. **A aplicação da tutela da proteção de dados pessoais no caso das portas interativas digitais do metrô de São Paulo.** 2019. Monografia. (bacharelado em direito) - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, Rio de Janeiro. Prof. Orientador: Flávio Alves Martins.

MALDONADO, N. Viviane.; BLUM, O. Renato. LGPD: **Lei Geral de Proteção de Dados: comentada.** 2ª edição. São Paulo: Revista dos Tribunais, 2019.

Portal Oficial Do Estado Da Bahia. **Reconhecimento Facial alcança 49 foragidos da Justiça no Carnaval.** Disponível em: https://www.bahia.ba.gov.br/2023/02/noticias/reconhecimento-facial-alcanca-49-foragidos-da-justica-no-carnaval/. Acesso em 14 set 2023.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Organização, seleção e apresentação de: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

A PRÁTICA DO SHARENTING, PROTEÇÃO DE DADOS PESSOAIS E O DIREITO À PRIVACIDADE DA CRIANÇA E DO ADOLESCENTE

Iana Santos Gonçalves Souza

RESUMO:

O presente trabalho disserta sobre a prática recorrente do sharenting, analisando as consequências da superexposição de imagens e dados de crianças e adolescentes pelos pais e sua contraposição ao direito à privacidade e à proteção de dados pessoais. Para tanto, será analisada a Lei Geral de Proteção de Dados Pessoais (LGPD), a interpretação do Enunciado CD/ANPD Nº 01/2023 no tocante a LGPD e o Estatuto da Criança e do Adolescente (ECA). Em suma, conclui-se que o sharenting tornou-se comum entre os responsáveis legais, sendo a prática normalizada e que estes não combatem ao compartilhamento de imagens excessivas dos menores sob sua tutela.

Palavras chave: Sharenting. Proteção de Dados. Criança. Adolescente.

1. INTRODUÇÃO

Ao longo do tempo, os meios tecnológicos conquistaram espaço essencial em todas as esferas da sociedade e resultaram em transformações importantes relacionadas, especialmente, ao crescimento das redes sociais. Segundo um levantamento realizado pelos países da América Latina, foi anunciado o Brasil como o maior consumidor de redes sociais, chegando a 356 bilhões de minutos gastos em plataformas digitais.

Junto ao advento dessas plataformas, o público infantojuvenil é apresentado

ao mundo digital cada vez mais cedo, ocasionando sua precoce exposição nas plataformas digitais. Nesse âmbito, inseridos no status de *influenciadores mirins*, muitas crianças e adolescentes se tornaram influenciadores digitais, sendo representados por seus pais ou responsáveis legais, que administram seus perfis nessas plataformas e gerenciam seu conteúdo. Essa situação, embora pareça inofensiva, revela inúmeras problemáticas, sobretudo no que diz respeito à alta exposição de crianças e adolescentes nas redes sociais. O compartilhamento de informações feitas pelos pais e responsáveis nas redes sociais é atribuído ao termo *sharenting*.

Deste modo, o presente trabalho tem como propósito analisar a exposição de dados pessoais de menores de idade, no contexto em que os pais e responsáveis legais compartilham, desmedidamente, suas informações na Internet. Procura-se discutir a proteção de dados pessoais e o direito à privacidade da criança e do adolescente, e assim, analisar quais medidas recorrer quando são feridos os seus direitos pela prática do sharenting.

2. O FENÔMENO DO SHARENTING

2.1. SHARENTING E PROTEÇÃO DE DADOS DAS CRIANÇAS NA INTERNET

Entende-se como *sharenting*, a união das palavras de origem inglesa "share", que significa compartilhar, e "parenting", que faz alusão a paternidade, mediante a execução do poder familiar. Como resultado, esse termo é utilizado para denominar a superexposição dos menores de idade na Internet, proveniente dos pais ou responsáveis legais, que compartilham fotos, vídeos e dados pessoais desses menores que estão sob o seu cuidado. Os pais e responsáveis, no entanto, não dão a devida importância às consequências futuras que podem provocar na construção da identidade da criança ou do adolescente, e muitas vezes extrapolam o limite e expõem momentos íntimos e vergonhosos dos menores, desrespeitando sua privacidade e provocando constrangimento, em certos casos, gerando, até mesmo, a sexualização dos menores.

Em consequência a era da informação e o desgovernado avanço tecnológico, o ordenamento jurídico brasileiro, como forma de proteger todos os indivíduos no meio digital, regulamentou a proteção de dados pessoais aos usuários, através, respectivamente, do Marco Civil da Internet e a Lei Geral de Proteção de Dados. Assim, destacam-se os direitos a serem resguardados pela norma jurídica, o respeito à privacidade e a proteção da imagem, intimidade e honra, dentro do ambiente digital.

Em especial, a Lei Geral de Proteção de Dados Pessoais (LGPD), discorre

sobre o tratamento de dados pessoais de crianças e adolescentes, a fim de protegê-los de abusos e violações de seus direitos. A LGPD, em seu artigo 14, exige para que o tratamento de dados dos menores de idade aconteça em seu melhor interesse, e, estabelece ainda, o consentimento específico de pelo menos um dos pais ou responsável legal do menor.

No que diz respeito ao sharenting, o fenômeno não é levado em conta no texto da lei e é totalmente deixado de fora, ignorado e não sendo citado em momento algum, o que coloca em risco a identidade da criança, inclusive, lesionando seus direitos, e, além do mais, podem ser observados brechas, abrindo espaço para diferentes entendimentos quanto ao uso dos dados desses menores. Percebe-se, então, que mesmo com sua atenção especial destinada ao tratamento de dados pessoais de crianças e adolescentes na Internet, a LGPD falha no que se refere à sua aplicação e efetividade.

Apesar disso, com o intuito de regularizar a interpretação sobre o tratamento de dados de crianças e adolescentes referente a LGPD, a Autoridade Nacional de Proteção de Dados (ANPD), trouxe, por meio do Enunciado CD/ANPD Nº 01/2023, o esclarecimento de que serão aplicáveis para o tratamento de dados de crianças e adolescentes todas as hipóteses legais previstas no art. 7º e art. 11º da LGPD, desde que prevaleça o melhor interesse do menor, a ser avaliado no caso concreto. Nesse sentido, o consentimento de pelo menos um dos pais ou responsável legal do menor deixou de ser a única hipótese legal adotada para o tratamento de dados de crianças e adolescentes, e deverá ser aplicado somente quando for a melhor hipótese legal ao caso concreto. Outras hipóteses legais, como a proteção à vida e as demais hipóteses previstas nos artigos indicados também serão aceitáveis.

2.2. SHARENTING E O DIREITO À PRIVACIDADE

Na Era Digital, as redes sociais ganharam um destaque inédito. Atualmente, plataformas digitais como Instagram, TikTok e YouTube dominaram o mercado, ocorrendo, dessa forma, a ascensão dos influenciadores digitais. Hoje, o que é postado nas redes sociais, milhares de pessoas ao redor do mundo têm acesso, se tornando quase impossível excluir, de fato, uma postagem, visto que há possibilidade de salvar postagens e capturas de telas, assim, não tendo controle do que poderá acontecer.

No tocante à privacidade, a exposição de menores que ainda não possuem capacidade para decidir atos por si mesmos, traz consigo inúmeras consequências. Um grave problema que pode ser iniciado é a erotização de crianças e adolescentes, quando os pais ou responsáveis legais provocam, imprevistamente ou não, a sexualização do púbere. Um exemplo desta questão se refere à cantora Melody,

também conhecida como MC Melody, a influenciadora mirim, atualmente com 16 anos, é vítima da hiper sexualização infantil desde os seus 8 anos, sofrendo com a adultização em suas redes sociais, desde fotos sensuais a participações em clipes de músicas erotizadas; seu pai, o responsável legal, foi investigado pelo Ministério Público por violar direitos envolvendo a dignidade da criança e do adolescente.

À vista disso, com a prática do sharenting, os infantes sofrem danos irreparáveis que violam os seus direitos fundamentais, uma vez que os responsáveis impedem que o menor desenvolva sua própria identidade. O Estatuto da Criança e do Adolescente (ECA), no seu artigo 17, é assegurado aos menores a inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, envolvendo o cuidado a imagem, identidade, autonomia, valores, ideias e crenças, dos espaços e objetos pessoais. Contudo, ao analisar o caso da cantora Melody, verifica-se que com apenas 8 anos, já havia fotos, dados pessoais expostos e postagens que corromperam sua imagem e violavam sua privacidade, fato este que a persegue até hoje na sua adolescência.

Outra vez, o ECA retoma seu papel em reafirmar os direitos da criança e do adolescente em seu texto, garantindo a dignidade e a privacidade para os infantes, são assegurados os mesmos direitos fundamentais garantidos aos adultos, pois também são sujeitos de direito e seus direitos necessitam de proteção. Entretanto, tendo em vista o cenário vivido atualmente, observa-se a violação rotineira desses direitos.

3. CONSIDERAÇÕES FINAIS

O presente trabalho surgiu acerca de um assunto extremamente importante e presente na sociedade contemporânea, entretanto é pouco abordado e demasiadamente normalizado.

Embora a Lei Geral de Proteção de Dados trate da questão da proteção de dados pessoais da criança e do adolescente, suas medidas são ineficazes e essa responsabilidade pertence, em grande parte, ao responsável legal do menor. Consequentemente, o Enunciado CD/ANPD Nº 01/2023 abrange as formas de tratamento de dados da criança e do adolescente, com fundamento nas hipóteses legais dos artigos supracitados.

Além disso, como fora visto, o direito à privacidade é garantido pelo Estatuto da Criança e do Adolescente. O caso citado da influencer mirim, Melody, é consequência do sharenting. Uma criança, que com apenas 8 anos, foi exposta e teve sua imagem e privacidade violadas, sendo vítima da hiper sexualização infantojuvenil.

4. REFERÊNCIAS

BRASIL. **Lei nº 13.709/2022 de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 set. de 2023.

FERNANDES, Cassiane Melo; FOLLONE, Renata Aparecida. **Proteção de dados pessoais da criança e do adolescente**. In: Anais do Congresso Brasileiro de Processo Coletivo e Cidadania. 2019. p. 1120-1139.

MORAES, Ana Carolina Ferreira de. **Sharenting e a proteção de dados e privacidade de crianças e adolescentes**. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 set. 2023.

BRASIL. Ministério da Mulher, da Família e dos Direitos Humanos. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União. ano 1990, Disponível em: https://cutt.ly/yECVBmB. Acesso em: 13 set. 2023.

ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes. Gov.br, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes> Acesso em: 11 nov. de 2023.

DADOS EXPOSTOS: UM PROBLEMA OU UMA VANTAGEM PARA A SOCIEDADE?

Mariana Amorim Mello

Atualmente, diante do grande desenvolvimento tecnológico e das inovações nas relações comerciais, bem como do estabelecimento e da aplicação de mecanismos digitais que contribuíram para uma maior efetividade dos serviços ofertados à população, surgiu a necessidade jurídica de regular essas conexões.

Desse modo, a LGPD (Lei n. 13.709 de 14 de agosto de 2018, que entrou em vigor em setembro de 2020) -Lei Geral de Proteção de Dados, estabeleceu ordem e parâmetros quanto à gestão dos dados do usuário, aspirando proteger a privacidade e a autonomia destes. Dessa maneira, determina preceitos para a reunião, o armazenamento, o tratamento e a divulgação dessas informações.

Entretanto, na contemporaneidade, a frequente divergência entre o direito público à informação e a privacidade aliada a segurança dos dados protegidos pela LGPD, revelou ser um problema para a sociedade.

Sob esse prisma, o direito ao acesso a informação, assegurado pela Lei nº 12.527/2011, positivada no dia 18 de novembro de 2011, define o acesso por parte da população as informações coletivas e a sua aplicabilidade pelos estados, Distrito Federal e municípios. A lei visa consolidar as políticas de transparência, mantendo a população constantemente informada.

Bem como o Artigo 5° da Constituição Federal, Inciso XXXIII, que consta: "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".

Concomitante ao pensamento do renomado filósofo e político inglês Francis

Bacon, conhecimento é poder. Dessa forma, o acesso as informações possibilita que a população crie juízo de valor sobre diversas questões, elabore um pensamento crítico e não seja manipulada por representantes do poder.

Em contrapartida, há o Artigo 5° da Constituição Federal que pode se relacionar simultaneamente com essa matéria, conforme o inciso II: "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" e o inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Isso destaca a importância do consentimento e da autorização do indivíduo para o compartilhamento de assuntos sobre os variados aspectos da sua vida.

Existe também as bases legais para o tratamento dos dados pessoais, que constam no Artigo 7° e 11° da Lei Geral de Proteção de Dados, que determina que a gestão dos dados pessoais não se limita ao consentimento do titular sobre os seus dados. Portanto, esse gerenciamento pode ser feito para o cumprimento de obrigação legal ou regulatória pelo controlador; execução de politicas publicas pela Administração; execução de contratos, exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física do titular ou de terceiro; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; proteção do crédito, inclusive quando disposto na legislação pertinente.

Assim, este problema é de extrema relevância em função do empasse de qual desses direitos deve prevalecer nas diversas situações que permeiam o cotidiano. Todos eles são positivados e legítimos e acabam se tornando opostos em muitos momentos, sendo difícil de conciliá-los.

Por conseguinte, surge um questionamento implícito no que tange o direito digital: o direito à intimidade e à vida privada juntamente com a necessidade do consentimento da divulgação dos dados do titular, devem prevalecer, ou, o direito de acesso à informação?

A título de exemplo, há a decisão do STF –Supremo Tribunal Federal- processo ARE 652.777, que decidiu favoravelmente sobre a divulgação de informação relativas aos servidores públicos na internet, entre elas os vencimentos, sob a perspectiva do conflito aparente de normas constitucionais. A discussão envolvia o direito ao acesso à informação de atos estatais, o princípio da publicidade administrativa, a privacidade, intimidade e segurança.

Assim, no acórdão, o município de São Paulo se posicionava de forma contrária às decisões judiciais que determinaram a retirada de informações do sítio

eletrônico. Sendo favoráveis à divulgação da remuneração dos servidores, seus cargos, funções e os órgãos de sua formação, destaca como fundamentação que o artigo 39, § 6º positiva a publicação anual do subsídio e da remuneração dos cargos e empregos públicos, revelando assim, não ter violação do direito à privacidade pois essas informações já estariam legalmente disponíveis.

Em suma, essa situação perpassou pela divergência dos direitos discorridos na presente dissertação: o da privacidade e consentimento dos servidores públicos em divulgar seus dados na internet e o direito fundamental de acesso à informação junto a possibilidade do tratamento e compartilhamento desses dados pela Administração Pública.

Nessa situação, houve o entendimento de que a prerrogativa do conhecimento dessa informação, vista como de interesse coletivo, deveria prevalecer sobre o da proteção dos dados do usuário do sistema financeiro e administrativo. Isso se justifica pela exceção no que tange a segurança pública assegurada pelo Inciso III do Artigo 7° da Lei Geral da Proteção de Dados.

Embora essa decisão seja apropriada, ela acarreta riscos para esses servidores, uma vez que, por terem seus vencimentos compartilhados, tornam-se alvos potenciais para propaganda intensiva e crimes como o sequestro extorsivo.

Para uma compreensão mais abrangente sobre o assunto e com o propósito de tentar solucionar esse conflito normativo, é imprescindível a realização de uma pesquisa mais aprofundada sobre alguns conteúdos. Isso inclui a analise da LGPD com o enfoque na questão da privacidade, consentimento e segurança dos dados do titular. Além das leis que tratam do direito à informação, as bases legais que legitimam o tratamento para além do consentimento e as situações em que há o conflito desses interesses: o de proteção à privacidade dos dados e o acesso à conhecimentos de domínio público. Também é necessário repensar o limite entre o consentimento do titular e o direito da publicização e do tratamento dos seus dados previstos pela LGPD nos casos concretos.

REFERÊNCIAS

https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProc essoEletronico.jsf?seqobjetoincidente=4121428

https://www.gov.br/capes/pt-br/acesso-a-informacao/servico-de-informacao-ao-cidadao/sobre-a-lei-de-acesso-a-informacao#:~:text=A%20Lei%20n%C2%BA%2012.527%2C%20sancionada,Distrito%20Federal%20e%20dos%20munic%C3%ADpios

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

https://www.jusbrasil.com.br/legislacao/612902269/lei-13709-18

O PETRÓLEO DO SÉCULO XXI

Raffael Simões Trindade de Medeiros

RESUMO:

A pesquisa visa trazer alguns pontos que devem ser expostos sobre os dados pessoais, o que são, como podem ser protegidos, como afetam a autonomia e a privacidade das pessoas. Além disso, busca se mostrar a forma errônea com que eles podem vir a serem usados por entes estatais e pelas Big Techs. Desse modo, provando a necessidade de se abordar esse tema cada vez mais cedo na vida do cidadão.

Palavras chave: Dados. Privacidade. Autonomia.

1. INTRODUÇÃO

Desde a criação dos primeiros computadores na década de 1970 até os atuais smartphones, nota-se que a tecnologia tem evoluído de forma exponencial nos últimos 50 anos. Isto trouxe bastante comodidade para vida das pessoas e diversos avanços em variados campos, como na medicina e engenharia.

No entanto, uma civilização cada vez mais conectada, fez com a sociedade passasse a ser movida pelos dados das pessoas. Este fato permite, em muitos casos, o domínio do Estado, das Instituições e das Big Techs sobre a vida do cidadão.

Assim, essa pesquisa tem como objetivo mostrar o porquê que é preciso que as pessoas cuidem muito bem dos seus dados pessoais e como o fazerem para que tenham sua privacidade e autonomia respeitada.

2. PRIVACIDADE, DADOS E PROTEÇÃO

Primeiro, deve se salientar que embora privacidade e proteção de dados sejam duas coisas distintas uma está fortemente ligada a outra. A primeira pode ser entendida como os temas da intimidade de qualquer um e que não estão sujeitos a serem acessados sem que haja autorização. Já a segunda como informações de uma pessoa, as quais podem ser de cunho privado ou público, e mesmo que sejam de caráter público isto ainda não dá o direito de qualquer ente fazer o que quiser com elas.

Então é perceptível que a privacidade e os dados pessoais estão muito ligados um ao outro. Por isso, a existência de legislações, que regulem o que pode ou não se fazer com o dado de outrem, é extremamente importante. Sendo essas regras a General Data Protection Regulation (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Entretanto, a autodeterminação informacional, que é a capacidade que o indivíduo tem de gerir seus próprios dados, torna-se limitada, por causa das leis. Isso ocorre, pois muitos dados serão de necessidade obrigatória de tratamento, por exemplo aqueles necessários para a Receita Federal. Ainda assim, essas situações estão expressas em um diploma disciplinar, algo que traz segurança jurídica, demonstrando a pessoa quais dados ela é obrigada a ceder, quais não são, qual a finalidade de tratamento, qual a necessidade dele, dentre outros.

Ademais, outro fato que precisa ser ressaltado é a diferença entre proteção de dados e privacidade de dados. Uma trata sobre a proteção de dados contra acesso não autorizado, a outra aborda o acesso autorizado em si, quem o tem e quem o define, respectivamente. Nesse caso, a segurança dos dados não garante a privacidade em si, já que a proteção dos dados será garantida pela tecnologia, ou seja, a capacidade do aparelho, no qual o dado está armazenado, em barrar ataques cibernéticos. Porém, a privacidade dependerá também da boa-fé do indivíduo autorizado a ter aquela informação mantê-la em sigilo e não só do aparato tecnológico que protege aquele dado.

Portanto, este último fato vai trazer a próxima discussão dessa pesquisa, que é a confiabilidade das grandes empresas e do próprio Estado. Esses atores, podem ou irão preservar os dados íntimos das pessoas, e caso não o façam, como isso pode afetar profundamente a autonomia e privacidade da vida dos cidadãos.

3. ATORES GLOBAIS, CONTROLE E PODER

A partir do que já foi dito anteriormente pode se dizer que a confiabilidade do agente de tratamento manter os dados pessoais em sigilo e fazer uso dele apenas para a estrita finalidade necessária é de suma importância para a proteção

da privacidade das pessoas. Todavia, em algumas situações, como as que serão abordadas nos parágrafos seguintes, essa boa-fé não foi respeitada e trouxe consequências que reverberaram fortemente na sociedade.

O primeiro caso é o da Cambridge Analytica, no qual dados pessoais de milhões de usuários armazenados no Facebook foram vendidos, sem autorização dos mesmos para tal, pela própria empresa para a Cambridge Analytica. Enquanto que essa fazia manipulações políticas a partir desses dados, sendo também a empresa de análise de dados que trabalhou com o time da campanha de Donal Trump em 2016. Tal situação mostra que a violação da privacidade não foi ocasionada pela falta de capacidade do Facebook de resistir a ataques cibernéticos, mas a irresponsabilidade criminosa de seus funcionários e da própria empresa. Já que, ela utilizou os dados para finalidades, que não foram autorizadas, lucrou com isso e ainda influenciou na escolha do presidente de uma das maiores potências mundiais. Logo, isso demonstra o poder que os dados das pessoas podem exercer quando usados estrategicamente.

Além disso, pode ser citado também, como outra exemplificação dessa problemática o Governo "Black Mirror" Chinês. Nele ocorre uma vigilância da vida dos cidadãos por instituições estatais que atribuem notas aos comportamentos de seus habitantes, podendo ceder vantagens aos comportamentos considerados benéficos e desvantagens aos interpretados como maléficos. Este tipo de experiência tem um potencial muito perigoso, uma vez que o Estado passa a controlar e monitorar, sem limites, a vida do indivíduo, o que torna muito difícil movimentos de oposição ao governo que está no poder. O tipo de comportamento supracitado é extremamente perigoso, porque é a partir do controle total da população, que um regime totalitário pode sedimentar suas bases de poder. Desse modo, pode-se inferir que a cautela em relação aos dados deve ir para além da Big Techs, pois caso haja um uso indiscriminado deles pelo governo, esse também é capaz de causar danos a privacidade e autonomia das pessoas.

Diante do que foi exposto anteriormente é possível afirmar que na atualidade os dados pessoais são o que o petróleo foi no século passado, ou talvez até mais valiosos. Uma vez que, além de serem extremamente lucrativos, são recursos que permitem os grandes atores do globo, dentre eles o próprio Estado e as empresas gigantescas do ramo de tecnologia, controlar e vigiar a vida das pessoas. Como resultado dá poder e controle imensuráveis a essas entidades, capacidade essa que é muito mais valiosa que qualquer outro tipo de riqueza na atualidade.

4. COMO PROTEGER OS DADOS

Após demonstrar anteriormente, o porquê de os dados pessoais serem valiosíssimos atualmente e como eles podem afetar a vida das pessoas negativamente se forem usados da maneira errada. A próxima questão seria, como fazer para

salvaguardar esse recurso em um mundo, onde as informações dos indivíduos são o principal combustível para diversos entes poderosos do globo. Então, a resposta para essa problemática é bastante complicada, pois embora legislações tenham sido feitas com o intuito de proteger os dados das pessoas. Percebe-se que seus efeitos não se provaram totalmente eficazes, como no caso da Cambridge Analytica, ou essas regras nem chegaram a ser criadas ou aplicadas em alguns locais do globo, a exemplo da situação "Black Mirror" do Governo chinês.

Diante disso, apenas é possível tomar precauções que amenizem essa questão, algumas delas poderiam ser: nunca dar informações pessoais que não sejam estritamente necessárias e com sua finalidade já explicada pelo agente de tratamento. Bem como, tomar muito cuidado com os provedores de internet de aplicação (sites, apps, redes sociais, entre outros) que se confia para armazenar os dados, sempre ler os termos de autorização de uso dos mesmos e ter senhas fortes para prevenir ataques cibernéticos. Além disso, evitar um excesso de terminais conectados à internet, como geladeira, máquina de lavar, smartwatches, dentre outros, pois embora tragam comodidade, também diminuem a privacidade da pessoa. Por fim, informar-se sobre a legislação que regulamenta a proteção de dados do seu país e quais são os seus direitos garantidos em lei.

5 CONCLUSÃO

Portanto, depois de tudo que foi apresentado nessa pesquisa é possível inferir que os dados pessoais são realmente o petróleo do século XXI. Devido a sua capacidade de manipular a vida das pessoas e permitir a vigilância da população, que é em sua maioria, descuidada com suas informações íntimas. Logo é de suma importância que essa problemática comece a ser abordada cada vez mais cedo na vida do indivíduo devendo ser matéria debatida desde a infância até a vida adulta. Afinal, a tecnologia evolui a passos largos e ao mesmo tempo que ela traz diversas vantagens ao mundo, também cria perigos avassaladores e a crescente falta de privacidade e autonomia da população é uma de suas maiores desvantagens.

REFERÊNCIAS BIBLIOGRÁFICAS

BARROS, Samuel De Jesus Monteiro De. **Evolução Tecnológica: um olhar para os últimos 50 anos.** Exame, 2023. Disponível em: https://exame.com/tecnologia/evolucao-tecnologica-um-olhar-para-os-ultimos-50-anos/. Acesso em: 04 set. 2023.

Privacidade de dados vs Proteção de dados. **ipswitch**, 2022. Disponível em: https://www.ipswitch.com/pt/blog/privacidade-de-dados-vs-protecao-de-dados. Acesso em: 04 set. 2023.

Privacidade e proteção de dados: entenda qual é a diferença. **Privacy Tech,** 2022. Disponível em: https://privacytech.com.br/protecao-de-dados/privacidade-e-protecao-de-dados-entenda-qual-e-a-diferenca,414166.jhtml. Acesso em: 04 set. 2023.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **g1**, 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: 05 set. 2023.

Black Mirror: cidade chinesa cria sistema de pontuação que premia e penaliza cidadãos. **globo.com**, 2019. Disponível em: https://epocanegocios.globo.com/Mundo/noticia/2019/04/black-mirror-cidade-chinesa-cria-sistema-de-pontuacao-que-premia-e-penaliza-cidadaos.html. Acesso em: 05 set. 2023.

A POSSIBILIDADE JURÍDICA DA REGULAMENTAÇÃO INTERNACIONAL DE DADOS NA INTERNET: UMA PONDERAÇÃO LUZ DA LEGALIDADE

Rebeca Ananias Pinto

1. CONTEXTUALIZAÇÃO DO TEMA E PROBLEMA DE PESQUISA:

O modelo de pesquisa utilizado nesse trabalho será o levantamento bibliográfico, a área de concentração é o Direito público, as disciplinas são Direito Internacional público e direito e tecnologia, o tema é "A possibilidade da da regulamentação jurídica internacional de dados na internet: uma ponderação luz da legalidade".

O artigo terá como objetivo analisar os fatores relacionados ao tema, como, quais são os principais debates e divergências doutrinarias que tocam a temática, desta forma, é imperativo analisar a origem do tema, com a evolução da regulamentação da internet em diversos países para assim alcançar a ponderação.

O enfoque do estudo é a interpretação dos "fenômenos" sociais e jurídicos que possibilitaram esse questionamento via compreensão da bibliografia produzida por doutrinadores, tendo destaque particular Malcolm N. Shaw no Direito Internacional, Soshana Zuboff no Direito e Tecnologia Internacional, Patricia Peck Pinheiro no Direito e Tecnologia brasileiro e Dirley da Cunha Júnior no Direito Constitucional Brasileiro e Direitos Fundamentais.

Analisando os países que se encontram mais avançados na regulamentação da internet e os efeitos disso nas redes sociais e na coleta de dados. É importante analisar regulamentações no âmbito nacional como a LGPD(Lei Geral de Proteção de Dados), assim como legislações de caracter transnacional como a RGDPR(Regulamento Geral sobre a Proteção de Dados) da União Europeia, e se existe a possibilidade jurídica da regulamentação internacional de dados na internet.

Ademais, levando em consideração os motivos particulares dessa circustância, como, por exemplo, que as empresas de Big Tech tem diferentes formas de lidar com o tratamento de dados a depender da legislação local, somado a outros fatores como uma proposta de tratado internacional pode ser realizada com países que tem entendimentos diferentes da importância e limites dessa regulamentação.

Diante do exposto, é imperativo questionar se essa possibilidade traria efeitos positivos ou negativos no esforço de combater as fake news e discurso de ódio, tendo em vista que um dos principais obstáculos é a falta de base de dados totalmente neutra nas redes sociais, algo que é intrinsecamente ligado a discriminação algorítmica e a necessidade de regulamentações precisas sobre governança algorítmica.

Por fim, é alcançado o seguinte problema de pesquisa, será analisado ao longo do artigo a possibilidade jurídica da regulamentação internacional de dados na internet, uma ponderação luz da legalidade, tendo como base os elementos sociais e jurídicos que estão no seu entorno, sendo fundamental a compreensão de que existem diferenças teóricas sobre o assunto analisado principalmente entres o setor privado e os Estados.

2. RELEVÂNCIA JURÍDICA E RELEVÂNCIA SOCIAL:

Ao ponderar sobre a relevância jurídica do tema de pesquisa do artigo, é importante entender que existe um alto volume transferencia internacional de dados na internet, mesmo que seja analisada apenas umas das grandes empresas de Big Tech ela tem capacidade de movimentar bilhões de dados de pessoas em qualquer lugar do mundo que tenha acesso a internet, sendo assim, esse um fenômeno de grande relevância jurídica por tocar a vida de quase toda a população global.

Entretanto, até o atual momento não existe uma regulamentação internacional sobre a internet, é primordial levar em consideração que os dados pessoais são uma grande de fonte de lucro, podendo ser considerados commodities não reguladas em escala internacional, tendo ligação direta com as redes sociais.

No sentido da análise, os direitos fundamentais, tem como características formar uma consolidação de direitos que tutelam os valores essenciais para assegurar condições de vida digna, tornam indispensáveis no intuito de formular a Democracia e Igualdade entre os povos, uma vez que são essências para a legitimação e organização da democracia, pois a dignidade do ser humano é a

origem e o último fito do sistema jurídico. Consequentemente, a dignidade da pessoa humana é um valor espiritual, moral e ético inerente a todos. O objetivo do artigo é justamente analisar a ligação entre relevância jurídica e relevância social do tema na luz dos direitos fundamentais, do direito internacional, direito digital e direito e tecnologia.

3. PROPOSTA DE PERCURSO DOS CONTEÚDOS:

Em primeiro plano, todas a descobertas, evoluções e quebra de paradigmas durante a história da humanidade, foram marcados por o desenvolvimento dessas novas realidades complexas no âmbito d direito que tem a capacidade de regulamentar de forma normativa as complexas relações do corpo social. A evolução da tecnologia atualmente ocorre mais rápido do que em qualquer outro período da humanidade, não apenas isso como também é inevitável que as pessoas em suas vidas hodiernas tenham o grande contato e em alguns casos dependência da tecnologia, com isso, é evidenciada a necessidade de analise da possibilidade jurídica da regulamentação internacional de dados na internet: uma ponderação luz da legalidade(DA CUNHA JÚNIOR, 2021, p. 53-56)

Não obstante, a revolução industrial 4.0 ao contrário das revoluções industriais anteriores não tem sua origem em bens tangíveis como o petróleo, aço ou maquinaria pesada, na verdade ela é marcada em sua configuração base por sua liquidez, alta rotatividade e velocidade, sendo desta forma por causa dessas características únicas considerado um capitalismo de vigilância, pois quem mais vai lucrar será o indivíduo, empresa ou conglomerado de empresas que tenha os melhores algoritmos que consigam captar o máximo de dados possível.

Em primeiro plano, tendo como base o artigo científico de Gabriel Ribeira Brega publicado na Revista de direito da FGV(BREGA, 2022, p. 3-7), durante o período dos últimos 20 anos o acesso à internet e a informação tornou-se mais fácil como nunca antes, o acesso em grande escala juntamente a algoritmos que visam o máxima manutenção do usuário na determinada rede social.

As empresas que formam a Big Tech precisam agir com maior responsabilidade e impor limites a disseminação do discurso de ódio e das notícias falsas(BREGA, 2022, p. 9), porém essa ainda não é a realidade temos como exemplo o Facebook e Google que tem como principal fonte de renda a venda de propaganda direcionada.

Tendo em vista essa problemática, a União Europeia aprovou em 2016 o "Regulamento Geral de Proteção de Dados" que entrou em vigor em 2018, priorizando os direitos dos cidadãos em oposição ao livre mercado digital. Já no contexto global ainda não possui tratados específicos referentes a proteção dos

dados na internet, apesar de existir debates crescentes de doutrinadores sobre essa possibilidade.

Outro aspecto fundamental é importância de entender que existe um alto volume transferencia internacional de dados na internet, mesmo que seja analisada apenas umas das grandes empresas de Big Tech ela tem capacidade de movimentar bilhões de dados de pessoas em qualquer lugar do mundo que tenha acesso a internet, sendo assim, esse um fenômeno de grande relevância jurídica por tocar a vida de quase toda a população global.

Destarte, com o grande influxo de transferencia internacional de dados na internet, mesmo que seja analisada apenas algumas das grandes empresas de Big Tech elas tem capacidade de movimentar bilhões de dados de pessoas em qualquer lugar do mundo que tenha acesso a internet, sendo assim, esse um fenômeno de grande relevância jurídica por tocar a vida de quase toda a população global.

Sendo importante analisar aspectos mais técnicos do assunto como a inexistência de uma base de dados neutra, em alguns casos a falta de neutralidade pode ocorrer de forma mais explícita, em outros casos não, como por exemplo empresas que não respeitam a data de validade dos dados, ou seja a data limite em que ela pode utilizar essa informação(PINHEIRO PECK, 2019, p.140-145).

Continuando, outra informação fundamental sobre o tema é a diferença entre os tipos de dados, dado pessoal não precisa ser necessariamente um dado cadastral, um dado pessoal pode ser uma foto ou um vídeo de determinada pessoa, e um dado sensível é, por exemplo, qual a sua filiação política, religião, sexualidade, se a pessoa é casada ou não(BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD), 13.709. 2018). Convém ressaltar que os diferentes tipos de consentimento coletados por empresas na internet, devem ser coletados de forma assim como organizados e armazenados separadamente, e caso o usuário não queira consentir isso não pode impedir ele de usar a plataforma.

Não obstante, dentro de um Terminal, que é considerado qualquer dispositivo que se conecta com a internet, as fontes dos algoritmos formam bancos de dados usando as informações para o "'machine Learning", desta forma, a máquina aprende um comportamento pré-estabelecido por seus criadores de como tratar as informações (CONCEIÇÃO,2018, p.9).

Por fim, é importante ressaltar que os sistemas tratados ao longo do texto precisam ser acessíveis, compreensivos e didáticos, desta forma, seria possível avançar na caminhada para alcançar a aplicação do princípio da governança algorítmica de modo regulamentado em escala mundial.

REFERÊNCIAS:

MALCON SHAW, **Internacional Law**, 2021, p. 787-813.

ZUBOFF, **Capitalismo de Vigilância**, 2021, p. 637.

PINHEIRO PECK, **Direito Digital**, 2019, p. 140-145, 481-490.

DA CUNHA JÚNIOR, **Curso de Direito Constitucional**, 2021. p. 53-56,554-564.

MAZZUOLI, **Curso Direito Internacional Publico, 2020, p. 243.**

BORGES, **Curso de Direito Internacional Público e Direito Comunitário**, 2011, p. 189-194.

KAPCZYNSKI, **The Law of Informational Capitalism**, 2020, p. 28.

BREGA, **A regulamentação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira**, 2022, 3-7, 9, 11, 15.

CONCEIÇÃO, **Globalização, Redes Sociais e hiper materialismo: O Direito Privado Voltado à proteção do consumidor como sujeito vulnerável na pós-modernidade**,2018, p. 9.

HARVARD LAW REVIEW, **Cooperation or Resistance? The Role of Tech Companies in Government Surveillance**, 2016, 130° Edição.

G1.GLOBO, Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/03/03/google-diz-que-deixara-de-vender-anuncios-com-base-no-historico-individual-de-navegacao.ghtml. Acesso em 23/03/2023.

THE NEW YORK TIMES, Disponível em: https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?referringSource=articleShare. Acesso em 29/03/2023.

G1.GLOBO, Disponível em: https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml. Acesso em 24/03/2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**, 13.709. 2018. Art. 52).

THE NEW YORK TIMES, When Algorithms Discriminate , By Claire Cain Miller, July 9 2015. Disponível em: https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?referringSource=articleShare

O IMPACTO DO TRATAMENTO DE DADOS NO CONSUMO CULTURAL: A IMPORTÂNCIA DO PLURALISMO NO ACESSO À CULTURA NO MUNDO DIGITAL

Rodrigo Lessa Fernandes Gallo

RESUMO:

O presente artigo tem, como objeto, a análise do impacto do tratamento de dados na forma como a sociedade consome cultura, debatendo a deficiência gerada pelos algoritmos e como a sua operatividade contribui de maneira negativa na diversidade cultural, ferindo o acesso à cultura estabelecido na Constituição Federal de 1998.

Palavras chave: Cultura. Proteção de Dados. Acesso à Cultura. Memória Cultural. Tratamento de Dados.

ABSTRACT:

The purpose of this article is to analyze the impact of data processing on the way society consumes culture, debating the deficiency generated by algorithms and how their operation contributes negatively to cultural diversity, harming access to culture established in the Federal Constitution of 1998.

1. O IMPACTO DO STREAMING NO CONSUMO CULTURAL

Com o avanço das tecnologias, a forma como se consome cultura mudou completamente nos últimos cinco anos. Se antes a nossa maior dificuldade era

encontrar um CD ou DVD específico nas diversas livrarias espalhadas pelo país, hoje conseguimos consumir qualquer mídia com apenas um clique. Os serviços de streaming se tornaram personagens essenciais dentro de uma sociedade que preza constantemente pela comodidade, possibilitando o consumo de uma quantidade exorbitante de mídia por um preço relativamente acessível.

Dentro da facilidade criada pelo streaming, ainda existe um coringa particular desses serviços: o algoritmo. Essa instrução de comandos criada para personalizar a experiência dos usuários dentro de uma plataforma possui um papel essencial no sucesso do streaming, desenvolvendo um catálogo quase exclusivo para quem assina e consome cultura dentro dos meios digitais. De acordo com seus gostos, o algoritmo trabalha para recomendar e expor apenas mídias que se encaixem dentro do seu padrão de consumo, chegando até a criar playlists com músicas que você nunca escutou, mas que provavelmente não vão sair dos seus fones por um bom tempo.

Toda essa comodidade, por mais incrível que pareça, possui preço praticamente invisível. Além de coletar nossos dados, algo que já se tornou comum na sociedade da informação, os serviços de streaming se utilizam dos nossos gostos para impulsionar conteúdos específicos, muitas vezes patrocinadospor grandes empresas, criando um ciclo de consumo difícil de se escapar.

É importante discutir o impacto desse consumo "domesticado" dentro de um país que enfrenta problemas para manter viva a sua memória cultural, seja pela falta de preservação dos órgãos competentes ou pelo simples esquecimento social decorrente à falta de publicidade que certas mídias possuem graças a enxurrada de conteúdos que navegam o nosso ambiente digital.

Qual foi a última vez que você consumiu, através de streaming, alguma mídia que fuja completamente do seus gostos? Até que ponto podemos dizer que o nosso acesso à cultura, mais ainda, à diversidade cultural, não se encontra viciado ou danificado por algoritmos? Qual é o papel desses serviços na proteção, preservação e divulgação da cultura e da nossa memória cultural? São questões que, ao meu ver, não possuem respostas exatas, mas que merecem um nível de indagação e atenção.

2. O ACESSO E PROTEÇÃO DA CULTURA DENTRO DO MEIO DIGITAL

De acordo com o art. 216 da Constituição Federal, os bens de natureza imaterial são considerados patrimônio cultural, fazendo com que qualquer mídia que se encontre armazenada no ambiente digital receba o mesmo nível de proteção e importância que uma obra física. As formas de expressão humana que

anteriormente só poderiam ser consumidas dentro de uma ótica material possuem agora uma versão imaterial, fazendo com que a aplicabilidade dos direitos culturais se torne maior e, consequentemente, englobando uma série de obras que só existem no plano digital.

A preservação do nosso acervo digital atravessa o simples cuidado de armazenamento, visto que preservar não é só manter vivo, mas também manter visto, acessível, para fomentar uma pluralidade cultural orgânica, onde todos podem descobrir e consumir diversos gêneros sem se prender a preconceitos.

No chamado mundo real, físico, não convivemos com um tratamento de dados cultural, um algoritmo que segura nossas mãos e que nos guia para algo pré-estabelecido. Antigamente, a descoberta artística era algo comum. A ideia de se perder em livrarias, sebos e locadoras, buscando e descobrindo novas obras que possuíam formas e aspectos que muitas vezes não dialogam nem um pouco com nossos gostos, mas que eventualmente se tornam um novo mistério a ser descoberto e decifrado por uma mente que foi desenvolvida para raciocinar e consumir cultura de uma maneira plural e democrática.

A existência do algoritmo, até certo ponto, dificulta drasticamente esseconsumo orgânico. A experiência da descoberta se tornou algo extremamente raro, visto que nos dias de hoje consumimos cultura dentro de um ambiente controlado, por uma ferramenta que afunila, com interesses próprios ou não, o que deve ser visto e o que deve ser consumido, muitas vezes apagando certas obras que não possuem um nível alto de visibilidade, contribuindo assim para um acesso precário à diversidade cultural.

O tratamento de dados dentro do consumo cultural, por mais que tenha entregue um nível de comodidade grande para a sociedade, desenvolveu um sistema que apaga consideravelmente a visibilidade de uma parcela significativa de obrasque devem ser descobertas e celebradas por uma grande variedade de públicos.

3. É NECESSÁRIO REGULAR O STREAMING? LGPD, PERSONALIDADE E CULTURA

A fundamentalidade dos direitos culturais é irrefutável, visto que se encontra no título Dos Direitos e Garantias Fundamentais da Constituição de 88, em seu Art. 5º, inciso LXIII, onde a carta magna define que a proteção dopatrimônio cultural é um direito fundamental de todos. A fundamentalidade de um direito mora na sua existência para a concretização da dignidade humana e para o desenvolvimento da personalidade de cada indivíduo. É impossível existir uma conexão genuína entre homem e sociedade sem esse direito, fazendo com que a

sua subsistência seja impedida graças à falta de garantia dessa faculdade.

É importante ressaltar que o reconhecimento de um direito fundamental atravessa o seu firmamento específico na norma, visto que a Constituição Federal,em seu Art. 5º, § 2º, sustenta que é possível identificar a fundamentalidade de um direito se ele carrega as mesmas características e princípios de um considerado fundamental pelo texto constitucional.

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu Art. 2º, VII, define que a disciplina da proteção de dados tem como um de seus fundamentosos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Ora, se a lei que regula o tratamento de dados no Brasil se baseia em um princípio que preza pelo desenvolvimento da personalidade, a mesma não deveria observar como esse tratamento impacta no desenvolvimento cultural da sociedade? Desenvolvimento esse que, como demonstrado acima, é um direito de personalidade defendido pela Constituição.

Por mais que o streaming se trate de um direito privado, a sua regulação, além de se basear nos princípios constitucionais, encontra também abertura no Art. 3º da LGPD, visto que de acordo com o mesmo, os princípios defendidos pelo Art. 2º se aplicam ao tratamento de dados realizado por pessoa jurídica, sendo de direito público ou privado.

A legislação já estabelece mecanismos acautelatórios para a proteção e impulsão do Patrimônio Cultural físico, material e imaterial, mas ainda não consegue enxergar e desenvolver ferramentas para proteger essas obras dentro do mundo digital. Por mais que o tempo e as outras formas de deterioramento físico não se apliquem ao meio virtual, a preservação dentro dessa esfera merece a mesma atenção, visto que o tratamento de dados e o desenvolvimento de algoritmos pode ser tão devastador para a nossa memória quanto as chamas de um incêndio.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14 de setembro de 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020).** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 14 de setembro de 2023.

SOBRE AS ORGANIZADORAS DESTES ANAIS

Christine Albiani

Advogada atuante em Compliance Digital e Proteção de Dados. Especialista em Direito Processual Civil e Direito Tributário. Certificada profissionalmente em Visual Law (CPVL) - Opice Blum Academy em parceria com a FGV Projetos. Graduada em Direito pelo Instituto Brasileiro de Mercado de Capitais (Ibmec RJ) com láurea acadêmica Summa Cum Laude. MBA em Gestão Tributária pela USP. Mestra em Direito pela UFBA. Autora do livro "Violação de direitos autorais e responsabilidade civil do provedor diante do Marco Civil da Internet". Integrante do 3º Grupo de Pesquisa do Instituto de Tecnologia e Sociedade (ITS-Rio) sobre Inteligência Artificial e Inclusão. Membra do Instituto dos Advogados da Bahia (IAB).

Maria Clara Seixas

Sócia da 4S Advocacia. Especialista em Direito Digital, IA Law, Proteção de Dados Pessoais, Governança Riscos e Compliance- GRC e Empresarial. Professora do INSPER, da Cubos Academy e Coordenadora do curso de LGPD e Privacidade da Faculdade Baiana de Direito. Pesquisadora em IA, Ética, Direito e Tecnologia e mestranda no tema pela UFBA. PDPP - EXIN Privacy & Data Protection Professional. Premiada como uma das advogadas mais admiradas do país em Direito Digital e Compliance pela Revista Análise Nacional e listada na Revista Compliance OnTop.

FACULDADE
BAIANA DE
DIREITO

FACULDADE BAIANA DE DIREITO E GESTÃO