

**XXX CONGRESSO NACIONAL DO  
CONPEDI FORTALEZA - CE**

**INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA  
E INTERNACIONAL**

**ANDRINE OLIVEIRA NUNES**

**EDITH MARIA BARBOSA RAMOS**

**RICARDO PINHA ALONSO**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

**Diretoria - CONPEDI**

**Presidente** - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

**Diretor Executivo** - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

**Vice-presidente Norte** - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

**Vice-presidente Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

**Vice-presidente Sul** - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

**Vice-presidente Sudeste** - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

**Vice-presidente Nordeste** - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

**Representante Discente:** Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

**Conselho Fiscal:**

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

**Secretarias**

**Relações Institucionais:**

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

**Comunicação:**

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

**Relações Internacionais para o Continente Americano:**

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

**Relações Internacionais para os demais Continentes:**

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

**Eventos:**

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

**Membro Nato** - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

I61

Internet: dinâmicas da segurança pública e internacional [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Andrine Oliveira Nunes; Edith Maria Barbosa Ramos; Ricardo Pinha Alonso. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-871-4

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 2. Dinâmicas da segurança pública e internacional. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34



# **XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL**

---

## **Apresentação**

Os trabalhos apresentados se relacionam com as pesquisas cuja temática envolve os estudos sobre a “Internet, dinâmicas da segurança pública e Internacional”. Foram apresentados no Grupo de Trabalho, no XXX Congresso Nacional do CONPEDI, em Fortaleza, no dia 17 de novembro de 2023 e renderam debates profundos e profícuos, valendo a leitura de cada linha e cada provocação que apresentam. Todos os temas apresentados, sob óticas distintas, deitam preocupação com a realidade que se impõe diante de todos, de vivermos diante de instrumentos tecnológicos fornecidos pela internet e as conexões que a rede proporcionou, com muitos efeitos positivos e, naturalmente, com outros que preocupam as sociedades modernas.

É necessário reconhecer que as relações pessoais, sociais, empresariais e públicas sofreram, nas últimas décadas, profundos impactos provenientes de sistemas e instrumentos tecnológicos e inovadores. E, tal movimento disruptivo contundia em curso como novas ferramentas surgindo a cada dia, a cada hora. A importância dos trabalhos apresentados é inegável na medida em que levantam questões relevantíssimas diante de novo e, em parte, desconhecido mundo em que vivemos.

Entre as pesquisas apresentadas, destaca-se a preocupação com a transparência ou a sua ausência, relativamente à inteligência artificial, cuja opacidade pode provocar impactos na segurança internacional, das relações entre Estados e Sociedades e produzir efeitos deletérios nos Direitos Humanos que exigem proteção especial nesse meio. Essa temática também rendeu outro trabalho, intitulado “O show de Truman e o fenômeno das fake news: A questão da regulamentação das redes sociais frente aos Direitos Fundamentais”. Isso demonstra que o tema, pela relevância, vem chamando a atenção dos pesquisadores. As fake News e as Redes Sociais, atraem olhares, tanto no que se refere à Ciência Jurídica, como também da Ciência da Informação.

Preocupações com os discursos do ódio também estão presentes, com pesquisa voltada à proposição de que a proibição de contas não autenticadas nas redes sociais pode servir como interessante ferramenta de regulação e de política pública para impedir desinformações, bem como evitar práticas abusivas.

A segurança dos dados que circulam nas redes também chama a atenção dos que pesquisam na área. Garantir que essas informações estejam protegidas efetivamente pode impedir que atos ilegais, crimes e mesmo comportamentos antidemocráticos sejam perpetrados nas redes e para além delas. Proteger dados e informações pessoais, sem dúvida impõe-se como medida absolutamente necessária.

Destaca-se também o trabalho que aborda a grande desigualdade que há entre aqueles que são submetidos a essa nova era digital, com potenciais prejuízos à democracia e liberdade de negociar livremente, com autonomia e compreensão efetiva das ferramentas tecnológicas, a permitir decisões e negócios livres e justos.

Os trabalhos são ricos e tratam com a devida profundidade questões de extrema importância teórica e prática da otimização das relações pessoais, negociais e profissionais no mundo que passa por constantes e abismais mudanças. Recomendamos, pois, vivamente, a leitura dos trabalhos.

# **A VIOLAÇÃO DA PRIVACIDADE DE DADOS COMO PROTAGONISTA DOS ATOS ANTIDEMOCRÁTICOS NO BRASIL**

## **THE VIOLATION OF DATA PRIVACY AS A PROTAGONIST OF ANTI-DEMOCRATIC ACTS IN BRAZIL**

**Polyana Marques da Silva  
Frank Sérgio Pereira  
José Sérgio Saraiva**

### **Resumo**

A presente pesquisa objetiva analisar o tratamento dos dados pessoais dos usuários pelas plataformas e nesse viés expor os modos pelos quais se dão as violações dos referidos dados no âmbito virtual. Nesse contexto, observa-se que em face da necessidade indissociável das ferramentas digitais na sociedade contemporânea, o uso irregular do dados e a consequente violação culmina num cenário em que vazamentos de dados tornam-se rotineiros e, por meio deles, práticas como disseminação de fake news se fazem presentes dentro das redes sociais. De tal modo, o trabalho visa expor o protagonismo da violação de dados frente aos atos antidemocráticos experienciados no Brasil recentemente, estabelecendo, ainda, a conexão entre a distorção de opiniões e a manipulação algorítmica veiculada aos meios digitais, em que mediante a coleta dos dados dos usuários é realizada a seleção de conteúdos específicos para determinado grupo, estando dentre estes as desinformações. Ademais, faz-se nítido que mesmo diante de legislação específica, sendo esta a Lei Geral de Proteção de Dados (LGPD), a questão da privacidade dos dados em ambiente virtual ainda carece de maior e mais ampla regulação, haja vista as omissões pelas quais os usuários estão expostos e os demais efeitos advindos da violação informacional, tal como os ataques à democracia.

**Palavras-chave:** Direito digital, Privacidade de dados, Violação da privacidade, Lgpd, Democracia

### **Abstract/Resumen/Résumé**

The present research aims to analyze the processing of users' personal data by the platforms and to explain the ways in which the violations of the aforementioned data are done in the virtual sphere. In this context, it is observed that in the face of the inseparable need for digital tools in contemporary society, the irregular use of data and the consequent violation culminates in a scenario in which data leaks become routine and, through them, practices such as the dissemination of fake news become present within social networks. Thus, the work aims to expose the protagonism of data violation in the face of the anti-democratic acts experienced in Brazil recently, establishing, also, the connection between the distortion of opinions and the algorithmic manipulation carried out to the digital media, in which through the collection of the data of users is made the selection of specific content for a particular group, being among these the desinformation. Moreover, it is clear that even in the face of

specific legislation, which is the General Data Protection Act (LGPD), the issue of data privacy in the virtual environment still needs greater and broader regulation, given the omissions to which users are exposed and the other effects arising from the breach of information, such as attacks on democracy.

**Keywords/Palabras-claves/Mots-clés:** Digital law, Data privacy, Violation of privacy, Lgpd, Democracy

## 1 Introdução

Com o expressivo avanço dos meios digitais na contemporaneidade mostra-se nítida a dependência da sociedade pelas suas ferramentas, tendo estas se tornado essenciais para o desenvolvimento das mais diversas atividades cotidianas, além de proporcionar aos usuários o comodismo de obter informações de forma fluída e instantânea. É inegável, assim, afirmar que as novas tecnologias trouxeram variados artifícios em benefício de seus usuários, diante de suas utilidades e facilidades proporcionadas.

Neste contexto, considerando ser impossível a mera possibilidade de desvinculação do indivíduo das plataformas digitais, são observadas problemáticas recorrentes em face de tal dependência. Assim, a violação da privacidade de dados encontra-se como sendo questão a ser atribuída atenção, uma vez que os dados pessoais dos usuários se constituem como seu direito fundamental, lhes sendo concedida a garantia de que suas informações sejam devidamente resguardadas no ambiente virtual, tendo em consideração que referidos dados possuem conteúdos sensíveis de seu detentor. Em muitos casos, tal violação se dá por meio do vazamento de dados nas plataformas ou pelo seu uso de forma indevida e, ainda, sem autorização.

Dessa forma, a presente pesquisa visa estudar a violação da privacidade de dados como protagonista dos atos antidemocráticos vivenciados no Brasil, uma vez ao se obter a posse dos dados pessoais de usuários das rede sociais, a realização de manobras políticas ilegítimas torna-se simples, fazendo com que a manipulação dessas informações trabalhem em favor de determinado fator em particular que, em suma, se mostra contrário aos ditames do Estado Democrático de Direito. Assim, é desempenhada uma análise crítica sobre os efeitos gerados pela violação da privacidade de informações pessoais, bem como explicitados os modos pelos quais referida garantia individual é lesada cotidianamente, além dos cenários já presenciados no país em decorrência de tal questão. Ademais, também será analisada a atuação da legislação brasileira frente a presente problemática, a fim de que seja possível expor os pontos carentes de regulação e, ainda, enunciar os projetos de lei que vem sendo estudados e as legislações estrangeiras que versam sobre a temática aqui pautada.

Não obstante, cabe salientar que para a construção do presente trabalho foi utilizado o método de abordagem dedutivo, que mediante o estudo de fatos gerais busca encontrar um resultado em específico, sendo este acerca do presente tema. Além disso, foram utilizados os métodos de procedimento histórico, estatístico e comparativo e ainda, foi feita a análise de legislações por meio do direito comparado. Nesse viés, adotou-se a pesquisa bibliográfica

como principal meio de pesquisa, sendo usadas como fontes livros, artigos e notícias que tenham conteúdo concernente com a temática do trabalho.

## **2 Objetivos**

A pesquisa tem por objetivo evidenciar a violação dos dados pessoais na esfera digital, a fim de expor o modo de tratamento e regulação das informações atualmente dentro das plataformas e, de modo crítico, explicitar as deficiências de suas políticas de privacidade e, ainda, do modo em que falta com transparência frente ao público.

Nesse viés, busca-se analisar os recentes atos antidemocráticos ocorridos no país por meio da análise da problemática da violação de dados, dada a sua utilização de maneira indevida em uma sociedade que faz o uso indissolúvel dos meios digitais, seja para receber ou difundir informações. Assim, faz-se mister a análise de atos como vazamento de dados, a fim de se estudar como os dados pessoais de uma massa de pessoas pode ser usada na manipulação de opiniões realizada por meio de disparos de *fake news* e, ainda, na manipulação do algoritmo em prol de determinado propósito do agente.

Por conseguinte, a presente pesquisa objetiva mapear a atuação da legislação vigente, tal qual a Lei Geral de Proteção de Dados (LGPD), além de comparar seus dispositivos com leis estrangeiras de mesma matéria, a fim de se obter um ponto de vista distinto do que já consta no país e, ademais, estudar os modos de contribuição dos dispositivos do PL 2.630/2020 para com a temática exposta. Vale salientar, que também é objetivo traçar possíveis novos caminhos regulatórios para a problemática que, ainda, carece de devida e eficaz regulação legislativa.

Deste modo, o principal objetivo é expor a problemática e a sua respectiva consequência dentro da sociedade, a fim de que possam ser evidenciadas possíveis medidas regulatórias para o ciberespaço e, ainda, a instituição de políticas que visem atentar os usuários acerca de seus direitos de privacidade no âmbito digital, em face do princípio da transparência.

## **3 A Privacidade de Dados Pessoais do Cidadão**

George Orwell em sua obra “1984” retrata uma realidade distópica em que a vida pessoal dos indivíduos eram observadas de forma constante por meio de uma tecnologia denominada “teletela”, não dispendo de nenhuma forma de privacidade, uma vez que era



impossível se desvencilhar da espionagem imposta. Não obstante, ao contrário do que observa-se na trama, pode-se afirmar que os cidadãos gozam do direito à privacidade sendo tal garantia indispensável para o devido exercício da liberdade individual, visto que mesmo diante um contexto público o indivíduo, por meio da sua privacidade, seleciona qual ato exarar publicamente. Dessa forma, é nítido que a privacidade é peça chave dentro do ambiente virtual que se encontra em constante ascensão, visto que:

No atual mundo digitalizado, como já ressaltado, o exercício do direito à privacidade será assegurado mesmo “em público”, não sendo mais limitado ao que não é exposto. A privacidade está presente mesmo quando há exposição, mesmo quando há compartilhamento da informação (Cancelier, 2017, p. 229).

A Lei Geral de Proteção de Dados Pessoais (LGPD), portanto, marca o início da regulação direta do uso dos dados pessoais no Brasil, pauta que anteriormente carecia de legislação própria no ordenamento jurídico do país, uma vez que “antes disso o Brasil contava somente com leis setoriais sobre proteção de dados” (Bioni, 2022, p. 60). Deste modo, a LGPD regulamenta o tratamento dos dados fornecidos pelos usuários às plataformas ou órgãos públicos, definindo limites para estes quanto a utilização das informações. Cabe salientar, aliás, que considera-se “dado pessoal” toda e qualquer informação que possa identificar o seu titular de algum modo, tal qual o número de algum documento ou até imagens e vídeos.

Nesse viés, pode-se observar que a instituição da Lei Geral de Proteção de Dados Pessoais (LGPD) trabalha a questão da privacidade de dados de maneira direta, suprindo o déficit legislativo outrora presente no país, trazendo em sua estrutura os requisitos a serem seguidos ao se trabalhar com informações pessoais, como a observância inescusável do consentimento de seu titular. Assim, a coleta dos dados pessoais somente se faz possível frente a anuência do detentor para o ato tornando-se, portanto, obrigação das plataformas requisitar tal consentimento para prosseguir com as suas atividades. De tal forma versa o inciso XII do art. 5º da LGPD, em que fica disposto que o consentimento se configura pela “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Brasil, 2018), sendo nítida que a responsabilidade sobre a utilização de tais dados por terceiros é transferida totalmente para seu respectivo titular.

Cabe salientar que, em tese, a privacidade de dados é direito de todo cidadão tendo este, por sua vez, o poder de consentir ou não sobre suas formas de utilização por terceiros o

que, no entanto, nem sempre é a realidade observada nos meios digitais. Em verdade, o que ocorre é que grande parcela das plataformas exige que o usuário conceda a permissão para a utilização de seus dados para que seja possível navegar por seus serviços, ao passo que se for negado o consentimento quanto às informações o usuário sequer consegue fazer uso das aplicações. Sendo assim, a “manifestação livre” da vontade do titular não se configura como inteiramente livre, uma vez que ao escolher não compartilhar seus dados, o indivíduo se vê limitado frente às ferramentas que lhes são apresentadas.

Dessa forma, é importante salientar que a liberdade individual é dada mediante o resguardo da privacidade, uma vez que por meio dela se faz possível a realização do livre arbítrio dos cidadãos, uma vez que cabe a cada um escolher o destino de suas próprias informações, sendo que:

[...] no Brasil, previsto tanto na Constituição quanto na legislação infraconstitucional, o direito à privacidade é considerado direito fundamental e direito da personalidade, sendo uma figura jurídica que supera a dicotomia entre direito público e privado (Cancelier, 2017, p. 222).

Não obstante, portanto, a privacidade de dados se constitui como direito fundamental do cidadão e é inerente para a devida efetivação de sua liberdade, visto que o direito de privacidade prioriza a vontade individual acerca da destinação e consequente utilização de suas informações. No entanto, no que concerne o âmbito virtual, encontram-se lacunas de transparência entre as políticas de dados das plataformas frente aos usuários e, ainda, é possível observar uma relação desequilibrada entre a convenção de consentimento entre as partes, uma vez que nem sempre são explicitados os modos pelos quais as informações serão efetivamente utilizadas pela plataforma ou, inclusive, a impossibilidade de uso de determinada ferramenta em virtude da não aceção dos termos propostos. Em face ao referido exposto, vê-se que claramente a privacidade de dados é posta numa espécie de “berlinda”, mesmo frente a LGPD que, justamente, tem por objetivo regular as relações que envolvam troca de dados, sendo tópico importante numa contemporaneidade em que o poder é direcionado àquele que detiver o maior volume de dados e informações.

### **3.1 As (Omissas) Políticas de Privacidade das Plataformas**

Em virtude do constante apego do ser humano pelos meios digitais e pelas redes sociais ali presentes, as “políticas de privacidade” ou “termos de uso” tornam-se expressões

populares na sociedade, uma vez que estes são disponibilizados ao usuário no momento em que realiza a inscrição em determinada aplicação digital, geralmente com o intuito de informar quais e como serão usados os dados fornecidos após a anuência do indivíduo em submetê-los à plataforma. Assim, pelos referidos meios é possível observar o dever da plataforma de fornecer as informações necessárias aos usuários que, por sua vez, como explicita Buoni (2022), possuem o direito de tomar conhecimento das características do serviço ali ofertado, bem como seus benefícios e malefícios.

Entretanto, importante ressaltar que o quesito da transparência nem sempre é demonstrado em sua totalidade diante do usuário que, por sua vez, ao consentir em fornecer os seus dados à plataforma mediante o aceite das políticas de privacidade apresentadas se vê lesado, levando em consideração a utilização de suas informações para finalidades distintas das pactuadas previamente. Além disso, é comum se observar a exclusão do indivíduo que não aceita os termos propostos da utilização dos serviços fornecidos, puramente pela negação em compartilhar seus dados pessoais com terceiros. É cristalino que as políticas de privacidade são, em verdade, omissas ao fornecer informações sobre a aplicação ao indivíduo, uma vez que é mais vantajoso para a empresa se abster em divulgar determinadas questões à seu público. Observa-se, dessa forma, que:

Deve ser assegurado aos usuários o acesso a essas facilidades do mercado, independentemente da existência de consentimento ou não, pois caso contrário à autodeterminação informativa se tornará letra morta da lei (Barreto Junior; Nascimento; Fuller, 2020, p. 11).

Nesse viés, observa-se que mesmo diante das disposições regulatórias da LGPD sobre a presente questão, a prática omissiva das plataformas permanece como realidade na sociedade, visto que no ramo virtual os dados pessoais passam a ter considerável valor econômico para aqueles que os detém, ou seja, as plataformas, ao monetizar o tráfego informacional criam um ambiente em que é estabelecida a realidade do mercado de informações (Buoni, 2022), sendo mais vantajoso omitir aos usuários a real destinação e quais dados em específico serão coletados no momento da concessão do consentimento, posto que, em face de tal cenário, a transparência poderia acarretar num maior número de recusas. Por conseguinte, vê-se que se o usuário não consentir com as políticas de privacidade propostas pela plataforma, muitas vezes, fica ele impossibilitado de fazer o uso das aplicações oferecidas pela empresa, haja vista que para ela não há nenhum ponto economicamente

proveitoso de ofertar um serviço sem, ao menos, poder se utilizar dos dados pessoais do indivíduo.

Não obstante, consta no artigo 9º da Lei Geral de Proteção de Dados, que é garantido ao titular as informações acerca dos modos em que seus dados vão ser utilizados, devendo constar de forma clara, corroborando com o princípio da transparência. De fato, são apresentados termos de uso e políticas de privacidade aos usuários previamente a sua inscrição nas plataformas, mas a transparência pela qual tais informações deveriam ser respaldadas são subjugadas em favor das redes, uma vez que:

Políticas de privacidade e termos de uso com textos longos e poucos claros não transmitem, na maioria das vezes, uma mensagem adequada para que o consumidor seja cientificado a respeito do fluxo dos seus dados pessoais. Ao revés, acaba por desinformá-los, trazendo ainda maior opacidade e assimetria de informações, desconsiderando, pois, o resultado ótimo/esperado de transparência que tal canal de comunicação deveria propiciar (Buoni, 2021, p. 161).

Deste modo, as plataformas adotam medidas que seguem as regulamentações acerca do dever de fornecer aos usuários os termos de uso mas, entretanto, é cristalino que tal obrigação é realizada de forma mascarada aos interesses privados do agente virtual, tendo os dados pessoais como principal vítima. Assim, pode-se afirmar que as omissões constantes nas políticas de privacidade podem ser consideradas postas ali de má-fé, em razão do valor econômico atribuído atualmente às informações pessoais, sendo possível, inclusive, relacionar o cenário aqui exposto à sociedade distópica de Orwell (2021), tratada no livro “1984”, com a diferença de que no atual contexto os dados pessoais dos cidadãos são tratados como mera mercadoria, em que as plataformas anseiam pela maior arrecadação possível, requisitando-os a todo momento, para a realização de qualquer movimentação dentro da internet, puramente para a sua própria ascensão.

#### **4. A Violação da Privacidade de Dados Pessoais**

A internet, nos dias atuais, é ferramenta indispensável no cotidiano da sociedade, tendo em vista os diversos mecanismos por ela disponibilizados e as facilidades que estes proporcionam. Em face do ambiente em que os meios digitais se fazem indissolúveis à vida humana, observa-se um alto e constante fluxo de informações dentro dos referidos meios, as quais encontram-se alocadas os dados pessoais dos usuários que usufruem das ferramentas. Ressalta-se que, como explica Zuboff (2020), ao fazer uso de qualquer sítio *online* em que

sejam fornecidos serviços e ferramentas gratuitas aos usuários, logo pode se concluir que, na realidade, tais mecanismos serão pagos como informações pessoais do indivíduo. Assim, nesta conjuntura, o que se encontram são empresas do ramo virtual usufruindo dos dados pessoais do público que, por sua vez, desconhece sua destinação final, mesmo lhes sendo garantido legislativamente o direito à transparência.

Os termos de uso e as políticas de privacidade, após a instituição da Lei Geral de Proteção de Dados (LGPD), tornam-se condições *sine qua non* para o funcionamento legal das plataformas virtuais no Brasil. Em contrapartida, os referidos termos são construídos de forma a omitir os modos pelos quais as informações fornecidas pelos usuários serão utilizadas. Em face de tal situação, o usuário se encontra enclausurado entre as opções de liberar seus dados ou ter o acesso à plataforma negado dado o não consentimento. Em face destas circunstâncias, é cristalino que os dados pessoais dos cidadãos são expostos de maneira que sequer é possível mensurar a quais atividades serão submetidos.

E é justamente neste viés que dá-se a ocorrência da violação dos dados pessoais, haja vista que as plataformas administram os dados de seus usuários da forma que mais lhe gerará proventos, sendo este uso indiscriminado considerado uma “infração da segurança que tenha por efeito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais” (Garrute; Schmidt, 2020, *online*), como disposto pelo art. 4º, item 12, do Regulamento Geral sobre a Proteção de Dados (GDPR), que regulamenta a proteção de dados na União Europeia. A Lei Geral de Proteção de Dados (LGPD), por sua vez, trata da problemática em seu art. 44, em que deixa explícito que haverá a violação de dados se a plataforma não seguir de acordo com as disposições legais ou não fornecer a segurança necessária aos dados pessoais do usuário (Brasil, 2018). Cabe salientar, no entanto, que mesmo diante do que é tratado pela LGPD no âmbito virtual brasileiro, a má utilização de dados pessoais se faz realidade, tendo em vista a cultura das políticas de privacidade omissas, o recolhimento de vultosas quantidades de informações visando lucro e, diante disso, o uso de dados para a geração de mais receita para as plataformas.

Insta ressaltar, ainda, que não é por acaso que as redes sociais são repletas de gatilhos que se enquadram nos padrões de cada indivíduo em particular, tal como observa-se com a aparição de conteúdos e propagandas correlatas à assuntos que são do interesse do usuário, mesmo que este sequer tenha realizado qualquer atividade ativa de busca àqueles conteúdos. O que ocorre, em verdade, é a coleta de dados do sujeito supracitado, sem que este ao menos tenha conhecimento mas que, ao mesmo tempo, concedeu consentimento à plataforma para que houvesse sua utilização mediante o aceite dos termos de uso, que por sua vez continha

informações omissas. É nítido, deste modo, que a violação dos dados é realizada com a anuência inconsciente do titular e, pode-se dizer, dentro do que define a legislação de dados, mesmo que a suposta garantia de transparência seja mais omissa do que esclarecedora sobre as reais intenções do que é requerido nos meios digitais.

#### **4.1. Vazamentos de Dados, *Fake News* e Atos Antidemocráticos**

Em face dos instáveis termos de uso de políticas de privacidade presentes nos meios digitais, é nítido que os dados pessoais dos usuários ficam expostos aos propósitos privados das plataformas que, por sua vez, se preocupam com a rentabilidade gerada pelo fluxo de informações. Diante de tal contexto, é comum se observar casos de vazamentos de dados pessoais em grandes plataformas digitais, tal como visto na empresa *Facebook*, em que no ano de 2018, por exemplo, fora confirmado o vazamento de dados de 87 milhões de usuários, sendo 443.117 destes de brasileiros (BBC, 2018). Observa-se que o vazamento de dados, que por si só já lesa o usuário, pode ser a porta de entrada para a ocorrência de diversas práticas inadequadas frente à sociedade.

Preliminarmente, importante frisar que, como supracitado, os dados advindos de vazamentos podem ser utilizados para os mais diversos fins, como para a manipulação de opinião de determinado grupo de indivíduos podendo ser, novamente, utilizado a plataforma *Facebook* a título de exposição da problemática. Shoshana Zuboff pontua o seguinte:

Vimos o conhecimento preditivo se transformando em poder instrumental nos experimentos de contágio do Facebook publicados em 2012 e 2014, quando inseriu sugestões subliminares e manipulou comparações sociais em suas páginas, primeiro para influenciar os usuários a votar nas eleições de meio mandato e mais tarde para fazer as pessoas se sentirem mais tristes ou mais felizes. Pesquisadores do Facebook celebraram o sucesso desses experimentos, observando duas descobertas: que era possível manipular sugestões on-line para manipular o comportamento e sentimentos do mundo real e que, ao mesmo tempo, isso poderia ser feito contornando a consciência do usuário (Zuboff, 2020, *online*, tradução nossa).

Nitidamente, o propósito da empresa é manipular as concepções populares, a fim de obter algum tipo de vantagem, como a maior constância em fluxo de utilização, tendo em vista que quanto mais tempo o usuário demandar dentro da plataforma, maior a quantidade de dados coletados e, conseqüentemente, maior o leque de geração de conteúdos perpendiculares aos seus interesses, em face da utilização de suas informações. É a partir daí que, por meio de dados pessoais mal administrados, vazamentos tornam-se a principal fonte de obtenção de informações para a realização de disparos de *fake news*. Tão grave é a situação que, inclusive,

no Brasil pode-se observar a atuação de uma gama de agências que coletavam os dados de cidadãos e, como visto no período eleitoral de 2018, ofereciam serviços de disparos de *fake news* para políticos que pagavam para que desinformações fossem espalhadas em favor de sua campanha. A jornalista Patrícia Campos Mello (2020, p. 55-56), atuante de forma ativa durante o período supracitado, traz relatos sobre a questão, expondo o ambiente, veja-se:

A Yacows oferecia em um site a venda de cadastros com milhões de números de celular atrelados a CPFs, títulos de eleitor, perfil social e econômico. A página da plataforma Bulk Services, pertencente à Yacows, anunciava como chamariz para a clientela “240 milhões de linhas de celular com perfil atrelado”; “100 milhões de títulos de eleitores”; “cruzamento de dados cadastrais com eleitorais”; “campanhas segmentadas por zona eleitoral” e “dados georreferenciados: por estado, cidade e bairros”. A página da Bulk Services não estava mais no ar, seu último registro havia sido em 18 de outubro de 2018, data em que a primeira reportagem citando a Yacows tinha sido publicada. Mas, como se sabe, é impossível apagar qualquer coisa da internet. A página pode ser acessada pelo link da Internet Archive, a Wayback Machine, espécie de arquivo oficial da internet. Ou seja: a agência não apenas usava CPFs para registrar seus chips, mas também oferecia a políticos bancos de dados. O meu e o seu número de celular, de título de eleitor e até nossa faixa de renda podiam estar à venda, sem nossa autorização.

Assim, a partir da coleta não autorizada e a respectiva venda de dados como nomes, CPFs, endereços e condições financeiras, fazia-se possível a determinação de temas relevantes para cada grupo de indivíduos (Mello, 2020), a fim de que fossem determinadas quais informações seriam enviadas para cada um, de modo a atingi-los de forma eficaz. Nesse contexto, em face do grande volume de desinformação política corrente nas redes sociais, há o exponencial crescimento de ataques aos princípios basilares do Estado Democrático de Direito vigente no Brasil, tendo em vista a manipulação realizada pela desinformação disseminada e, ainda, pela incidência da idolatria a figuras políticas, advinda justamente da corrente de *fake news*, que alia-se ao fenômeno da pós-verdade. Vê-se, deste modo, que um problema é responsável por uma longa sequência de desdobramentos que aflige um único ponto, a democracia do país.

Faz-se mister salientar que a questão não se restringe apenas aos parâmetros digitais, partindo com violência para as estruturas públicas físicas do Brasil. O uso indevido dos dados pessoais, culmina em vazamento de dados que, por consequência, deságua na venda de informações sensíveis, disparos de *fake news* e manipulação da concepção popular acerca de temáticas já enraizadas. Com isso, inclusive, importante mencionar que as distorções de informações direcionadas à determinado público alvo, que no início do ano de 2023 foram presenciados ataques aos prédios dos Três Poderes em Brasília, em que por meio de atos violentos era tentado se alcançar a anulação dos resultados da eleição do ano anterior, tendo

em vista a derrota do candidato que anteriormente ocupava o cargo presidencial. Tal candidato, aliás, contribuiu diretamente para o ocorrido, uma vez que este se valia das plataformas digitais para publicar e influenciar seu público a acatar informações desconexas com a realidade, com vistas ao seu benefício próprio. Acerca do ocorrido em questão, houve a divulgação entre os apoiadores do candidato de que o artigo 142 da Constituição Federal poderia levar a interpretação de que a uma intervenção militar se faria possível caso fosse da vontade da população. A referida *fake news* foi uma das principais responsáveis pelos atos antidemocráticos observados no país, tendo em vista que uma informação distorcida compartilhada dentre grupos específicos de indivíduos fora tida como verdade absoluta, mesmo que o conteúdo do documento constitucional seja claro acerca da impossibilidade de qualquer intervenção ao regime vigente.

Dessa forma, é cristalino que a violação da privacidade de dados contribui para que atos antidemocráticos tornem-se fatos recorrentes no Brasil, haja vista que mediante a utilização indevida dos dados pessoais dos usuários é realizada a manipulação de opiniões e a distorção de informações em face de disputas políticas. A manipulação culmina em atos antidemocráticos, sendo nítido que a problemática vai além da utilização não consentida dos dados pessoais, que por meio de diversas manobras, tal qual o vazamento e posterior venda, tornam-se protagonistas na desestabilização do regime democrático estabelecido no país.

#### **4.2. A Manipulação Algorítmica**

Em face das distorções de informações supracitadas, é importante mencionar a influência algorítmica das redes sobre seus usuários acerca da percepção da realidade absorvida por meio do conteúdo recebido e consumido pelos meios digitais. Os algoritmos, deste modo, se constituem como a tecnologia responsável por selecionar e direcionar conteúdos aos usuários baseando-se em suas movimentações *online*, se tornando “cada vez mais poderosos, pois possuem a capacidade de aprender através de exemplos” (Pellizzari; Barreto Junior, 2019, p. 59-60).

Nesse viés, observa-se que o grande fluxo de dados aliados à coleta indiscriminada destes pelas plataformas digitais, tendo em vista o consentimento “forçado” concedido pelo usuário ao concordar com os termos de uso e políticas de privacidade, corroboram de forma direta para atuação eficaz dos algoritmos dentro dos aplicativos. Assim, os algoritmos atuam de forma a agrupar indivíduos que possuam os mesmos interesses, mediante a sugestão de



seus perfis uns entre os outros, além de direcionar publicações, publicidades e serviços conexos às pautas de interesse.

É possível afirmar, por um lado, que o referido mecanismo de enquadrar como uma funcionalidade útil no meio virtual, uma vez que facilita o acesso do usuário aos conteúdos que são do seu agrado. Entretanto, o que se observa é atuação algorítmica contribuindo com a disseminação de desinformação e a manipulação de opiniões, ou seja, “o uso de filtros informacionais desenhados pelo algoritmo, potencializam o acirramento de dois fenômenos alienadores contemporâneos, as *fake news* e a pós-verdade” (Pellizzari; Barreto Junior, 2019, p. 62). Deste modo, fica claro que a partir dos dados fornecidos pelos usuários às redes sociais este torna-se, automaticamente, sujeito a receber informações inverossímeis e, ainda, ser influenciado a permanecer dando engajamento a elas, além de realizar suas próprias publicações a despeito da temática. Ademais, tal exposição não só gera efeitos inatos, como é causador de condutas ativas dos grupos afetados, como se observou nos ataques às estruturas dos Três Poderes e com as correntes de discursos antidemocráticos defendidas fielmente por considerável parcela da população.

Não obstante, sobre a óptica das plataformas a utilização dos dados para as referidas finalidades somente importam para o seu retorno econômico, uma vez que quanto maior o fluxo de informações nas redes, maior o ganho das plataformas e é deste modo que descreve Zuboff (2020, *online*, tradução nossa) ao pontuar que o “capitalismo da vigilância começa a reivindicar unilateralmente a experiência humana privada como matéria-prima para a tradução em dados comportamentais. As vidas são representadas como fluxo de dados”. Ainda neste viés, Zuboff (2020) detalha que foi construída uma barreira entre as tecnologias das plataformas e seus anseios por capital frente aos efeitos gerados na sociedade contemporânea. Por conseguinte, o sociólogo Bauman (2001, p. 17) versa sobre a presente realidade, defendendo que “é a velocidade atordoante da circulação, da reciclagem, do envelhecimento, do entulho e da substituição que traz lucro hoje - não a durabilidade e confiabilidade do produto”. Faz-se nítido, portanto, que os interesses privados das plataformas virtuais vem se sobressaindo aos direitos de privacidade resguardados aos cidadãos que, por sua vez, têm informações que lhes são de direito omitidas.

## **5. As Possíveis Abordagens Frente às Violações de Dados**

Como visto, a privacidade de dados no âmbito digital é uma temática que influi sobre diversos fatores, desde a garantia fundamental do cidadão às estruturas do Estado

Democrático de Direito do país. As plataformas são munidas de grande poderio, ainda mais frente ao valor atribuído aos dados dos usuários e a exposição ao qual estes são sujeitos em favor das grandes empresas virtuais. Deste modo, uma vez que a internet é ferramenta indissolúvel para a sociedade nos dias atuais, faz-se nítida a disparidade de tratamento entre o direito à privacidade e a forma pelas quais as informações dos indivíduos são utilizadas pelas plataformas haja vista, inclusive, que tais informações são tidas como mercadoria.

Em face de tal contexto, a Lei Geral de Proteção de Dados estabelece em seu art. 7º inciso I, que a transferência de dados pessoais somente poderá se realizar mediante o consentimento livre e expresso de seu detentor, atribuindo-lhe o direito de gerir suas próprias informações. Entretanto, o que se observa é a omissão das plataformas no que concerne ao tratamento destes dados e, ainda, a impossibilidade de uso de seus mecanismos caso o consentimento lhe seja negado. Observa-se que há uma clara lacuna na LGPD sobre a referida questão, uma vez que ao disponibilizar de forma prévia aos usuários os termos de uso e as políticas de privacidade, mesmo que omissas ou com conteúdos de difícil compreensão popular, as empresas do ramo digital se encontram nos limites, em tese, dos ditames da legislação, subjugando o direito à privacidade de dados pessoais do usuário, visto que “não adianta atentá-lo sobre algo que lhe é útil, se o conteúdo informativo não é completo suficiente para nela desencadear uma compreensão completa, e, por último, racionalizar uma tomada de decisão - poder de decisão” (Bioni, 2022, p. 146).

A LGPD tem por objetivo dar ao cidadão o direito de gerir seus próprios dados por meio de disposições que lhe garantam uma relação transparente com as plataformas, traçando regulamentos específicos para estas o que, no entanto, é feito de modo superficial, sendo escassas as possibilidades de interpretação trazidas em seu texto. É essa superficialidade, inclusive, que se beneficiam as empresas privadas haja vista que:

[...] não se faz necessário o acesso ao dado pessoal detalhadamente, com a finalidade de espionar os dados do indivíduo, mas por meio da identificação de padrões de aprendizado, apreendidos a partir do processamento de grandes quantidades de dados é possível prever, mesmo que com margem de erro, o comportamento dos usuários online (Molina; Barreto Junior, 2022, p. 268-269).

Destarte, evidencia-se que a atual conjuntura legislativa constante no Brasil é vantajosa para as empresas privadas do ramo digital, na medida em que a capitalização dos dados pessoais em face da coleta facilitada gera inestimáveis benefícios às plataformas. A chamada “autodeterminação informativa” é o direito do titular de decidir sobre a destinação de seus dados pessoais e respectivo tratamento (Molina; Barreto Junior, 2022), direito que por

sua vez é manipulado em favor dos interesses particulares já explicitados. Em vista disso, é cristalina a necessidade da adoção de complementações à Lei Geral de Proteção de Dados, a fim de que esta exerça a devida eficácia sobre o atual cenário. Assim, se atentando ao Regulamento Geral sobre a Proteção de Dados (RGPD), como explica Buoni e Mendes (2022) é presente a ferramenta dos relatórios de impacto à proteção de dados pessoais:

[...] pelos quais o controlador - quem tem poder de tomada de decisão na cadeia de tratamento de dados - deve obrigatoriamente executá-los quando houver um *alto risco em jogo*. A regulação europeia, além de trazer uma lista exemplificativa dessas situações, exige que os órgãos fiscalizadores sejam comunicados apenas quando o próprio agente econômico não encontrar meios de mitigar os prováveis malefícios da sua respectiva atividade, devendo nesse caso aguardar “luz verde” da autoridade para seguir em frente (Buoni; Mendes, 2022, p. 382-382).

A LGPD, por sua vez, também determina a elaboração de um documento que deve descrever as formas de tratamento de dados adotados pelas plataformas, como dispõe seu art. 5º, inciso XVII (Brasil, 2018), mas não é constatada nenhuma exigência em face de atividades de alto risco, diferentemente do que é disposto pela regulamentação europeia. Ademais, outro ponto importante trabalhado pela RGPD é a questão da comercialização de dados pessoais, em que de acordo com seu art. 21 item 2 e 3, se observado o uso das informações do usuário para fins de obtenção direta de lucro, fica resguardado a ele o direito de revogar a permissão concedida à plataforma, o que é abordado pela LGPD de forma mais sucinta, visto que a questão da capitalização dos dados não é pautada.

Com vista ao exposto, a legislação brasileira de proteção de dados se faz de suma importância no presente contexto de avanços dos meios digitais e a respectiva necessidade humana intrínseca à seus mecanismos. Entretanto, mesmo diante de suas disposições ainda são observadas carências de regulação na LGPD, sendo possível a implementação de novas disposições que visem complementar seu corpo. Além disso, os usuários encontram-se em posição desigual às plataformas, visto que não possuem acesso à todas as informações que lhes são de direito, sendo por meio de medidas que visem informar e educar a população que se alcançará uma maior paridade de direitos e obrigações entre as partes. Deste modo, pode-se afirmar que a transparência é a principal responsável por estabelecer a harmonia na relação do tratamento dos dados pessoais no ambiente virtual, sendo essencial para o presente contexto.

## **6. Considerações Finais**

Com as funcionalidades fornecidas pelos meios digitais, seu uso torna-se inerente às necessidades da sociedade contemporânea que, por sua vez, busca cada vez mais praticidade e rapidez para as atividades cotidianas. Em face de tal contexto, as aplicações digitais demandam de forma progressiva o acesso aos dados dos indivíduos, definindo como requisito indispensável para a permissão de utilização de seus serviços, mesmo que seja resguardado ao usuário o direito à privacidade e, ainda, a chamada autodeterminação informacional.

O que ocorre, em verdade, é que mesmo diante às claras garantias dos cidadãos e às disposições trazidas pela Lei Geral de Proteção de Dados, os dados pessoais dos usuários são tratados pelas plataformas como mercadoria num cenário em que o fluxo informacional é alto e constante, sendo realizadas manobras para que mediante termos de uso e políticas de privacidade omissas, seja possível afirmar que é oferecida transparência em face ao público, mesmo que na realidade o que se observam são textos confusos de linguagem complexa e a “coação” para a concessão de consentimento feita quando o usuário é restringido de fazer uso da ferramenta por não compartilhar suas informações.

Em face deste cenário e, ainda levando em consideração a manipulação algorítmica intrínseca às redes digitais e a capitalização dos dados pessoais, a manipulação de opiniões e distorção de temáticas torna-se realidade no país, em que mediante o uso exacerbado das plataformas digitais passa a se observar reações antidemocráticas e atos de agressões ao patrimônio físico do Brasil em razão dos conteúdos consumidos *online*, que ali são dispostas justamente para agradar este público em específico, a fim de que passem mais tempo utilizando os serviços e, conseqüentemente, gerando mais lucro à empresa responsável por gerir tais dados.

Deste modo, é nítido que apesar das inúmeras novas possibilidades e facilidades trazidas pela era digital, são muitos os pontos que carecem de atenção, tendo em vista o direito à privacidade e o respectivo direito de liberdade que do primeiro culmina, uma vez que cada indivíduo deve ter o controle sobre seus próprios dados e tal controle somente poderá ser realizado se forem oferecidos os meios propícios para tal. Ademais, é nítido que a ambição das empresas do ramo digital em gerar lucros vai além aos ditames do Estado Democrático de Direito e as reações populares frente a ele, dada a enxurrada de desinformação compartilhada por meio de suas ferramentas. Fazem-se necessárias intervenções frente ao cenário explicitado, a fim de que universos distópicos como “1984” de Orwell não se tornem uma realidade mesmo que, de fato, o grande irmão do mundo real contemporâneo são as plataformas que atuam de todos os modos para favorecerem a si próprias, uma vez que a

legislação hoje vigente é passível de brechas em seu texto e a população exposta aos termos e políticas que não resguardam a sua privacidade.

## Referências

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001.

BARRETO JUNIOR, Irineu Francisco; NASCIMENTO, Ariane Azevedo Carvalho do; FULLER, Greice Patrícia. Lei Geral de Proteção de Dados: Efetividade Jurídica do Consentimento do Titular para Tratamento de Registros. **Revista de Constitucionalização do Direito Brasileiro**, [s. l], v. 3, n. 2, p. 1-23, 2020.

BIONI, Bruno *et al* (org.). **Proteção de Dados: contexto, narrativas e elementos fundantes**. São Paulo: Câmara Brasileira do Livro, 2022.

BBC. **Facebook Admite Uso Indevido de Dados de 87 Milhões de Usuários, 443 mil no Brasil**. 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43646687>. Acesso em: 19 set. 2023.

BRASIL. Lei nº 13.709, de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade Hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, p. 213-239, 2017.

EU. Regulamento 2016/679, de 2016. **Regulamento Geral sobre a Proteção de Dados (RGPD)**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504>. Acesso em: 21 set. 2023.

GARRUTE, Mateus Mello; SCHMIDT, Estela. **A violação de dados pessoais e seus impactos sob a égide do Regulamento Europeu de Proteção de Dados (GDPR)**. 2020. Disponível em: <https://www.migalhas.com.br/depeso/319059/a-violacao-de-dados-pessoais-e-seus-impactos-sob-a-egide-do-regulamento-europeu-de-protecao-de-dados--gdpr>. Acesso em: 19 set. 2023.

MELLO, Patrícia Campos. **A Máquina do Ódio: notas de uma repórter sobre fake news e violência digital**. São Paulo: Companhia das Letras, 2020.

MOLINA, Fernanda Zampieri; BARRETO JUNIOR, Irineu Francisco. Capitalismo de plataforma: a ameaça ao direito à autodeterminação informativa na sociedade da informação. **Revista Brasileira de Estudos Políticos**, Belo Horizonte, n. 125, p. 243-278, 2022.

ORWELL, George. **1984**. Rio de Janeiro: Antofágica, 2021.

PELLIZZARI, Bruno Henrique Miniuchi; BARRETO JUNIOR, Irineu Francisco. BOLHAS SOCIAIS E SEUS EFEITOS NA SOCIEDADE DA INFORMAÇÃO: ditadura do algoritmo e entropia na internet. **Revista de Direito, Governança e Novas Tecnologias**, Belém, v. 5, n. 2, p. 57-73, 2019.

ZUBOFF, Shoshana. **You Are Now Remotely Controlled: surveillance capitalists control the science and the scientists, the secrets and the truth**. Surveillance capitalists control the science and the scientists, the secrets and the truth. 2020. Disponível em:

<https://www.nytimes.com/2020/01/24/opinion/surveillance-capitalism.html>. Acesso em: 18 set. 2023.