

DA VIGILÂNCIA DIGITAL NO CONTEXTO DOS DIREITOS HUMANOS E DO DIREITO À PRIVACIDADE

RESUMO: Na sociedade digital, na qual os indivíduos estão cada vez mais conectados ao mundo virtual, os dados individuais são coletados e processados diuturnamente. A prática de apropriação da experiência humana para o monitoramento indiscriminado, tanto das empresas quanto dos governos, é uma afronta aos direitos humanos e, em especial, ao direito à privacidade, inclusive no contexto escolar. Para defender as garantias fundamentais, este trabalho visa entender o fenômeno da vigilância digital no contexto do direito à privacidade, utilizando o método dedutivo, partindo da análise bibliográfica e legislativa.

PALAVRAS-CHAVE: direitos humanos, direito à privacidade, coleta de dados, sociedade digital, vigilância digital.

ABSTRACT: In the digital society, in which individuals are increasingly connected to the virtual world, individual data is collected and processed day in and day out. The practice of appropriating human experience for comprehensive monitoring, both by companies and governments, is a counter to human rights and, in particular, the right to privacy. To defend fundamental guarantees, this work aims to understand the specificities of digital surveillance in the context of the right to privacy, using the deductive method, based on bibliographic and legislative analysis.

KEYWORDS: human rights, right to privacy, data collection, digital society, digital surveillance.

1 INTRODUÇÃO

Em meio as inovações tecnológicas e transformações sociais enfrentadas pela sociedade contemporânea, o fenômeno da vigilância ganhou novos contornos e tornou-se um tema central e controverso. Com a difusão de dispositivos conectados à internet e o avanço das tecnologias de coleta e análise de dados, a capacidade de monitorar atividades individuais e coletivas atingiu níveis preocupantes. Assim, não há mais limites de “paredes” ou tempo para se perpetuar a vigilância. Neste artigo, essa prática será denominada “vigilância digital”, pois a tecnologia estabeleceu um novo paradigma e, portanto, viu-se uma necessidade numa nova abordagem do assunto.

A discussão sobre a vigilância digital tornou-se imperativa, visto as muitas violações ao direito à privacidade e a necessidade de se construir barreiras jurídicas de proteção as garantias fundamentais do homem, inclusive em ambiente escolar. Como o fenômeno levanta questões cruciais sobre privacidade, segurança e liberdade, o estudo do tema se torna essencial a construção de conhecimento acadêmico, para

que, assim, futuramente possam ser elaboradas medidas assertivas quanto a proteção de direitos inerentes ao ser humano.

A presente pesquisa tem como objetivo geral possibilitar a compreensão do fenômeno da vigilância digital no contexto dos direitos humanos e do direito à privacidade. Os objetivos específicos são os seguintes: analisar e conceituar o direito à privacidade, com ênfase na dignidade da pessoa humana, no direito de personalidade e na sua nova faceta: o direito à proteção de dados; e explicar a vigilância digital, contextualizando-a na sociedade digital e examinando suas implicações nos setores público e privado. Vale ressaltar que este trabalho não pretende esgotar o assunto, nem tem a pretensão de resolver todos os problemas decorrentes da vigilância, mas sim trazer luz ao tema.

Para conduzir esta pesquisa, será utilizada a metodologia científica dedutiva com revisão bibliográfica, buscando uma análise crítica e abrangente das obras e estudos existentes sobre o assunto.

2 DO CONTEÚDO JURÍDICO DO DIREITO À PRIVACIDADE

A privacidade é tutelada pelos direitos humanos no contexto da ascensão da tecnologia de informação. Por isso, este capítulo focará no direito à privacidade e nos novos desafios que esta garantia enfrenta no presente. Para atingir este objetivo, serão analisados os pilares da dignidade da pessoa humana e sua relevância na garantia do desenvolvimento da personalidade. Posteriormente, será delineado o conceito de privacidade e introduzida sua faceta mais recente: o direito à proteção de dados pessoais.

2.1 Dignidade da Pessoa Humana e Direito de Personalidade

Com a evolução do Direito, reconheceu-se o homem como centro do ordenamento, e, para protegê-lo, foram feitos os Direitos Humanos, esses tendo como fim a promoção da dignidade da pessoa humana. Ainda é desafiador estabelecer precisamente um conceito à dignidade da pessoa humana, dificuldade certamente proveniente da multiplicidade de sentidos do termo e também por estar sempre em constante construção a medida que sociedade se desenvolve. Apesar da dificuldade,

Sarlet atribui um adequado conceito:

Assim sendo, temos por **dignidade da pessoa humana a qualidade intrínseca e distintiva reconhecida a cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade**, implicando, neste sentido, um complexo de direitos e deveres que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de **propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência** e da vida em comunhão com os demais seres humanos, mediante o devido respeito aos demais seres que integram a rede da vida (2015a, p. 70-71, grifo nosso)

Nesse mesmo liame, a dignidade da pessoa humana é definida por Bobbio (2002, p. 54) como “um princípio que possui características de irrenunciabilidade e intransmissibilidade e retrata o reconhecimento de que o indivíduo há de constituir o objetivo primacial da ordem jurídica”. Para positivar esse entendimento, a Constituição Federal Brasileira de 1988 firmou logo no início de sua Carta (Art. 1º, inciso III) a dignidade da pessoa humana como sendo um dos fundamentos da República Federativa Brasileira. De modo que se tornou inequívoco a intenção do legislador originário em destacar esse princípio como fundamento da ordem jurídica.

Assim, para tutelar o valor intrínseco do ser humano e dar mais tangibilidade à sua dignidade, foi-se criado uma série de direitos específicos que hoje são abarcados nos chamados “direitos de personalidade”. O estudo dessa teoria de direitos de personalidade é essencial para entender o papel do direito na formação e desenvolvimento do ser humano. Garantir os direitos de personalidade é garantir que cada pessoa tenha liberdade para sua autodeterminação.

Nesse passo, para entender melhor sobre a personalidade:

a personalidade consiste no conjunto de caracteres próprios da pessoa.[...]A personalidade é que apoia os direitos e deveres que dela irradiam, é objeto de direito, **é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é**, para sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens (TELLES JR, apud. DINIZ, 2024, p. 50, grifo nosso).

Ainda com os ensinamentos de Maria Helena Diniz, o direito da personalidade seria o direito de defender a vida, a liberdade, a imagem, a privacidade, a honra e tudo que lhe é próprio; de modo que se pode exigir um comportamento negativo dos outros para se proteger. Tais direitos “são absolutos, intransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis e inapropriáveis” (DINIZ,

2024, p.50).

Assim, entende-se que a violação de qualquer um dos direitos de personalidade é uma violação direta da dignidade da pessoa humana. Mais adiante, mostrar-se-á evidente a importância de se proteger os direitos à privacidade como forma de proteção da personalidade do indivíduo.

2.2 Do Direito à Privacidade

A tarefa de estabelecer um conceito sempre encontra reverses e é passível de erros, no entanto, é um processo essencial. Como Kant, na obra "Crítica da Razão Pura", aduz "Todo conhecimento exige um conceito, por mais imperfeito ou obscuro que ele possa ser" (2001, A106). Isso não é diferente quando se trata da privacidade, visto ser um direito fundamental para a dignidade humana e a autonomia individual, logo, é complexo e multifacetado, apresentando diversas nuances.

Na análise da temática, percebe-se uma ampla gama de conceitos relacionados ao direito à privacidade. Cada um desses conceitos destaca um aspecto específico desse direito. Além disso, com as mudanças sociais, surgem novas interações, resultando em novos aspectos da privacidade, como é o caso do Direito à Proteção de Dados, inclusive no âmbito das escolas e demais instituições de ensino.

Na teoria tridimensional da privacidade, defende-se a ideia de que em "uma violação da privacidade, na verdade, o que se está querendo dizer é que ocorrem várias violações, em vários direitos da personalidade" (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 35-56). Essa teoria divide a privacidade em três dimensões: espacial, decisional e informacional. A espacial é a mais tradicional dimensão da privacidade, correspondendo a um determinado lugar físico, por exemplo, um cômodo da casa. A decisional está ligada à proteção da escolha do modo de vida do indivíduo, incluindo seus gostos e crenças (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 35-56). Por último, a dimensão informacional se relaciona intrinsecamente com a proteção de dados pessoais, visto que envolve a proteção de informações pessoais.

Ademais, Tércio Ferraz (1993) explica que o direito à privacidade é um direito subjetivo fundamental e, por isso, manifesta-se numa estrutura em que os elementos são: o sujeito, o conteúdo e o objeto. O sujeito é o titular do direito, por ser um direito fundamental, o sujeito será qualquer pessoa, física ou jurídica, brasileira ou

estrangeira, residente no País. O conteúdo da privacidade, como direito, é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio. O objeto é o bem protegido, sendo a integridade moral do sujeito.

Em seguida, Ferraz traz interessante reflexão para o estudo do tema. Ele afirma que a ideia de privado é dominada pelo princípio da diferenciação e exclusividade, pois, de outro modo, não seria possível desenvolver indivíduos autônomos e livres. O princípio da exclusividade foi cunhado pela filósofa alemã Hannah Arendt com base em Kant e “visa a assegurar ao indivíduo a sua identidade diante dos riscos proporcionados pela niveladora pressão social e pela incontrastável impositividade do poder político” (FERRAZ, 1993, p.3).

Desse modo, para que seja obedecido o princípio da exclusividade, são necessários três atributos: a solidão, que seria a faculdade de estar só; o segredo e a autonomia. Isso pode incluir a solidão como espaço para reflexão e autodescoberta. O segredo, como forma de proteger aspectos íntimos da vida. E a autonomia, como poder individual de decisão não forçada. Portanto, a exclusividade refere-se àquilo que é singular e pessoal, resultante das escolhas individuais que não são determinadas por normas ou padrões, mas sim pela subjetividade e liberdade do indivíduo. De modo que sempre visa “um mesmo propósito: a integridade moral do indivíduo, aquilo que faz de cada um o que é e, desta forma, lhe permite inserir-se, na vida social e na vida pública” (FERRAZ, 1993, p.5).

A constituição brasileira versa sobre a privacidade em seu art. 5º, inciso X, e declara invioláveis a intimidade e a vida privada:

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; (PLANALTO, 2024, grifo nosso)

Por conta dessa diferenciação que o texto constitucional traz entre intimidade e vida privada, parte da doutrina buscou uma definição para cada um dos termos. Ferraz define intimidade como

é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum) (FERRAZ, 1993, p.4)

Em seguida, define a vida privada como:

Já a vida privada envolve a proteção de formas exclusivas de convivência.

Trata-se de situações em que a comunicação é inevitável (em termos de relação de alguém com alguém que, entre si, trocam mensagens), das quais, em princípio, são excluídos terceiros.(FERRAZ, 1993, p.4)

Desta forma, a doutrina e a Constituição Federal Brasileira reconhecem a privacidade como um direito fundamental que estabelece um espaço de autonomia individual, onde o indivíduo não precisa dar explicações sobre suas escolhas e comportamentos para terceiros, a não ser por desejo ou consentimento do indivíduo.

Levando em consideração os conceitos abordados, cabe aprofundar-se em uma das mais novas facetas do direito à privacidade: o direito à proteção de dados.

2.3 Do Direito à Proteção de Dados

O espaço virtual representa uma parcela significativa do cotidiano contemporâneo. Todos os dias, informações são geradas e coletadas nesse lugar. Essas informações muitas vezes consistem em dados pessoais que por natureza são sensíveis e vulneráveis e devem ser protegidos. Por conta disso, diversos países criaram legislações específicas para a proteção dos dados pessoais.

Os primeiros debates sobre o tema foram realizados pela União Europeia (UE), momento em que surgiu o Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), esta lei tratou de assuntos como proteção de dados, privacidade e intimidade de indivíduos, além da livre circulação de dados, conhecido pela expressão "*free data flow*".

No âmbito legislativo nacional, é importante lembrar que haviam algumas legislações para regular a internet. O Código de Defesa do Consumidor e a Lei do Comércio Eletrônico (Lei nº 7.962/2013), por exemplo, permitia ao consumidor acessar seus dados pessoais e de consumo e reconheceu os dados como um bem jurídico.

A proteção de dados ganhou um contorno mais abrangente com o Marco Civil da Internet (Lei 12.965/2014), que não se limitou a um tipo específico de dados, mas generalizou a proteção à privacidade no ambiente digital, assegurando direitos como o consentimento explícito para a coleta e tratamento de dados, a clareza nas informações sobre a utilização dos dados pessoais e o direito à exclusão dos mesmos.

Porém, foi apenas com a Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018, que se tutelou de forma concisa e objetiva no que se refere aos critérios que são considerados adequados para o processamento, armazenamento e

descarte desses dados. A inovação da Lei consistiu em estabelecer um padrão para os atributos qualitativos da proteção de dados pessoais, definindo critérios claros e penalidades para quem os infringissem, o que também se aplica as escolas.

Apesar dos avanços na legislação de proteção de dados, ainda se enfrenta desafios significativos na garantia da privacidade na era digital. A rápida evolução tecnológica, a coleta excessiva de dados e as práticas de vigilância em massa representam ameaças constantes à privacidade dos indivíduos.

3 DA VIGILÂNCIA DIGITAL DIANTE DO DIREITO À PRIVACIDADE

Num *podcast* feito na plataforma *Youtube*, Elon Musk - fundador das empresas Tesla Motors, SpaceX e Neuralink - afirmou acreditar que a maioria das pessoas da atualidade já podem ser consideradas ciborgues (PowerfulJRE, 2018). O dono de algumas das maiores empresas de tecnologia argumentou que o *smartphone* se transformou numa extensão do corpo humano, tornando-o dependente. Apesar da impactante declaração, é inegável a dependência das pessoas com seus dispositivos de celular. Afinal, o aparelho substituiu boa parte das ferramentas usadas para lidar com o cotidiano. Agora, esse dispositivo, através de seus aplicativos, tornou-se o relógio, a agenda, o banco, o mercado, o entretenimento, o modo de localização (*GPS*), o meio de comunicação e, a cada dia, surgem mais funções.

No ambiente de trabalho não seria diferente, visto que é difícil se pensar numa atividade laboral sem qualquer interferência da tecnologia. Os indivíduos utilizam-se de computadores e o chamado "sistema" das empresas para realizar suas demandas. No lazer, as pessoas recorrem mais uma vez ao digital para se entreterem, fazendo uso de redes sociais, *streaming*, jogos eletrônicos e mesmo livros digitais.

De fato, é impossível dissociar o ambiente físico do virtual, de forma que as pessoas vivem em uma "Sociedade Digital". Manuel Castells também descreve essa realidade como "sociedade em rede" e esclarece o desenvolvimento desse novo modo de vida ao mencionar que, por volta de 1970, emergiu um novo paradigma tecnológico fundamentado na tecnologia da informação. Esse paradigma causou um impacto tão significativo "que concretizou um novo estilo de produção, comunicação, gerenciamento e vida" (CASTELLS, 2002, p.43).

Fazer parte disso não é mais uma escolha dos indivíduos, mas uma realidade.

Afinal, não estar inserido no meio digital significa ser excluído de boa parte da vida em sociedade. É nesse universo digital que se encontra majoritariamente oportunidades de trabalho e amiúde exige-se habilidades quanto a tecnologia. Encontra-se também serviços governamentais e privados, como bancos, educação, saúde e serviços públicos. Inclusive, é fonte de intensa interação social e troca de informação e notícia. De modo que, as pessoas são coagidas a estarem cada vez mais conectadas, sob ameaça de serem excluídas na “nova realidade”.

3.1 Da Vigilância Digital

Com o advento da Sociedade Digital, paralelo a uma miríade de facetas deste tempo, surge o fenômeno da Vigilância Digital. A vigilância em si não é algo novo, visto que é um fato social observado anteriormente, como nos casos mencionados do paóptico e do *Big Brother*. Mas, conforme destaca David Lyon, as modernas infraestruturas de tecnologia da informação, que possibilitam o processamento em tempo real e o armazenamento ilimitado de dados, não apenas aprimoram a vigilância, mas trazem uma mudança “qualitativa” à vigilância (LYON, 1994, p.40).

Um traço marcante da vigilância contemporânea, que a distingue dos modelos discutidos por Foucault e Orwell, é sua sutileza e imperceptibilidade. Enquanto as vigilâncias descritas por esses autores eram visíveis e rígidas, facilitando a resistência, a vigilância de hoje ocorre de maneira mais discreta, tornando a oposição mais difícil e tendente a criar servos dóceis. Observa-se hoje uma presença “amigável” da vigilância principalmente por parte das empresas privadas. Nessa linha, David Lyon aduz:

Envolve autopolicimento descentralizado; mais uma vez, notamos acima como participamos na nossa própria monitorização. Isso desencadeia uma mudança da identificação de suspeitos específicos para uma suspeita categórica. É mais intensivo e mais extenso. Na metáfora de Stanley Cohen, a rede é mais fina, mais flexível e mais larga (LYON, 1994, p. 53, tradução nossa).

A vigilância digital surge da premissa de que a vida na sociedade digital gera dados. E, segundo Shosana Zuboff (2021), todas as ações dentro dela são registradas, guardadas, transmitidas, tratadas e transmitidas novamente para atender interesses dos que a possuem. Assim, o fluxo de informação de dados pessoais se expande afetando pontos da vida cotidiana e traz uma preocupação quanto ao “fim da

privacidade”.

Sob tal perspectiva, Elias Jacob de Menezes Neto esboça, baseando-se em David Lyon, um conceito de *surveillance*, aqui chamada de Vigilância Digital:

Ela é a atenção concentrada, sistematizada e rotineira aos dados pessoais cujo objetivo é influenciar, gerenciar, proteger ou dirigir. Concentrada, pois seus alvos finais são, via de regra, os indivíduos. Sistematizada, uma vez que essa atenção não é aleatória ou ocasional: é deliberada e depende de determinados protocolos e técnicas. Rotineira, porque “normalizada”, ou seja, compreendida como parte inescapável do cotidiano em todas as sociedades atuais, uma vez que dependem da associação crescente entre a tecnologia da informação e a administração burocrática. Logo, a *surveillance* é um fenômeno onipresente nas sociedades contemporâneas (JACOB NETO, 2014, p. 7).

Um fator para a expansão da vigilância digital é a capacidade de coletar informações de forma descentralizada. Essa capacidade envolve a coleta e processamento de dados em múltiplos pontos ou dispositivos, em vez de centralizar todas as operações em um único local ou sistema. O exemplo mais proeminente é a Internet das Coisas (IoT). Dispositivos IoT, como sensores ambientais, *wearables*, dispositivos domésticos inteligentes e carros conectados, estão equipados com a capacidade de coletar dados diretamente de seus ambientes operacionais. Estes dados podem ser processados localmente ou transmitidos para a chamada Computação em Nuvem que permite que dados sejam armazenados e processados em servidores remotos.

Junto a isso, Jacob Neto aborda o fenômeno conhecido como "*Dataveillance*", um termo que combina "*data*" (dados) com "*surveillance*" (vigilância) e descreve a prática de monitorar e coletar dados digitais sobre indivíduos ou grupos sem qualquer critério (JACOB NETO, 2014, p.11). Essa ação evidencia a falta de um propósito predefinido para a Vigilância Digital. Esse fenômeno se tornou um desafio em termos de privacidade e direitos fundamentais, pois permite um nível de observação e análise detalhada que é muitas vezes é invisível para os sujeitos dos dados e pode ser usada de maneiras que afetam negativamente a autonomia e a liberdade individual.

3.2 Da Vigilância Digital no âmbito privado

Uma das formas de se utilizar a vigilância digital é o que foi chamado por Shosana Zuboff de “Capitalismo de Vigilância”. Segundo a autora, o capitalismo de vigilância se caracteriza pela apropriação unilateral da experiência humana como

matéria-prima gratuita para a geração de dados comportamentais (ZUBOFF, 2021). Esses dados, extraídos das atividades diárias dos indivíduos em plataformas digitais como Google, Facebook e Amazon, são usados não apenas para melhorar produtos e serviços, mas principalmente para criar previsões sobre comportamentos futuros.

Essas empresas se utilizam da Mineração de dados (*data mining*), que consiste num processo de descobrir padrões, correlações ou *insights* em grandes conjuntos de dados utilizando métodos que abrangem estatística, análise de dados, e aprendizado de máquina. Essencialmente, é uma técnica usada para extrair informações valiosas de dados, que de outra forma seriam difíceis ou impossíveis de analisar devido ao seu volume, variedade e velocidade. Coletados e tratados esses dados, as empresas podem vender as informações pessoais para outras corporações que tenham interesse em adquiri-los. Este processo, aparentemente técnico, tem implicações éticas profundas, pois transforma a vida pessoal em *commodities* para serem comercializadas.

Há incontáveis exemplos de como essa e outras técnicas de vigilância são empregadas pelo setor privado para impulsionar o consumo. Segundo *global overview report* (2022), a *Meta Platforms, Inc*, é um conglomerado americano que administra três das maiores redes sociais do mundo — *Facebook, Whatsapp e Instagram* —, e exemplifica bem isso. Essa empresa construiu seu vasto patrimônio oferecendo serviços gratuitos que se tornaram parte da vida contemporânea. Em contrapartida, ela coleta dados de seus usuários, processando essas informações para criar um sistema de previsão altamente preciso, vendido a anunciantes que buscam maximizar seus alcances (FORBES, 2023).

Zuboff conceitua como capitalismo de vigilância:

[...] O capitalismo de vigilância **reivindica de maneira unilateral a experiência humana como matéria-prima gratuita** para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superavit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de previsão que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses **produtos de previsões são comercializados num novo tipo de mercado para previsões comportamentais que chamo de mercados de comportamentos futuros**. [...](Zuboff, 2021, p.21, grifo nosso).

O conceito de vigilância, que outrora evocava imagens de estados totalitários e controle explícito, agora é percebido nas práticas cotidianas de empresas que se intrometem na vida privada sob o disfarce de conveniência. E evidente a natureza invasiva da coleta de dados pessoais pelos gigantes da tecnologia que frequentemente ocorre sem o consentimento explícito dos usuários ou com um entendimento limitado. As políticas de privacidade são muitas vezes propositadamente complexas e confusas, dificultando que os usuários compreendam e controlem suas próprias informações. Enquanto as empresas detêm o conhecimento e a capacidade tecnológica para extrair e analisar dados em grande escala, os usuários ficam à mercê de suas práticas, muitas vezes sem recursos adequados para contestar ou optar por não participar.

Portanto, o capitalismo de vigilância, ao transformar a privacidade em produto e o comportamento humano em mercadoria além de comprometer o direito à privacidade, também interfere no desenvolvimento da personalidade, na autonomia individual e desafia os princípios democráticos fundamentais de liberdade e autodeterminação. É vital que se desenvolvam novas formas de regulação e resistência a essas práticas para garantir que os avanços tecnológicos sirvam para promover o bem-estar humano, e não apenas para aumentar os lucros das corporações.

3.3 Da Vigilância Digital realizada pelo Poder Público

Como já abordado, a prática de monitoramento dos indivíduos pelo poder público não é uma novidade. Porém, com a ascensão da sociedade digital e o avanço tecnológico, essas práticas alcançaram uma dimensão global. Sob a justificativa de proporcionar maior segurança aos seus cidadãos e a "guerra ao terror", governos implementam e expandem seus programas de vigilância.

Por causa dos acontecimentos conhecidos como "11 de setembro", países aprovaram legislações Antiterrorismo que ampliaram os poderes das agências de segurança para monitorar comunicações e coletar informações sobre indivíduos como, por exemplo, o USA PATRIOT Act dos EUA (2001). Essas leis frequentemente permitem que as agências de inteligência e segurança conduzam vigilância, desde a coleta massiva de dados de comunicações até o uso de câmeras de vigilância e reconhecimento facial em espaços públicos. Essas práticas são frequentemente conduzidas sob pouca ou nenhuma transparência, deixando cidadãos sem saber quais

dados são coletados, como são armazenados, processados ou compartilhados.

O emblemático caso Edward Snowden, ocorrido em 2013, mostrou ao mundo a vigilância exercida pelos Estados Unidos através da *National Security Agency* (NSA), a Agência de Segurança Nacional norte-americana. Antes das revelações, Snowden trabalhou para a CIA e como contratado em várias organizações de defesa e inteligência, o que lhe deu acesso a informações altamente classificadas. Então decidiu levar ao conhecimento geral o fato de que o governo norte-americano, sob a justificativa de garantir a segurança do país contra o terrorismo, interceptou as comunicações eletrônicas não apenas de suspeitos, mas de pessoas, autoridades e instituições de vários países. Os documentos vazados revelaram que a NSA utilizava de programas de alta tecnologia - PRISM, Upstream2 e XKeyscore – que a permitiam acessar dados de grandes empresas como Google, Facebook e Apple. Como se não bastasse, eram capazes de acessar quase todo o tráfego mundial da internet (GREENWALD, 2014).

As consequências jurídicas desses eventos ainda não podem ser compreendidas em sua totalidade. Contudo, Daniel Solove aborda as implicações da vigilância estatal desregulada de uma forma que ressalta como isso pode transformar a estrutura do poder social. De acordo com Solove, a capacidade do estado de acumular e analisar grandes quantidades de dados sobre seus cidadãos sem as devidas restrições e supervisões coloca-o em uma posição de poder que pode ser profundamente desequilibrada em relação aos cidadãos (SOLOVE, 2015).

Hoje, o governo tem uma fome sem precedentes por dados pessoais. Está a explorar os dados detidos por empresas e outras organizações, incluindo bibliotecas. **Muitas empresas atendem prontamente às solicitações de dados do governo.** As agências governamentais estão a explorar estes dados pessoais, tentando determinar se uma pessoa poderá provavelmente envolver-se em atividades criminosas ou terroristas no futuro, com base em padrões de comportamento, compras e interesses (O'Harrow 2005). **Se um computador do governo decidir que você é uma ameaça provável, você poderá acabar em uma lista de observação, poderá ter dificuldade para voar e poderá haver outras consequências negativas no futuro** (SOLOVE, 2015, p.71, tradução nossa)

Quando o governo tem acesso a informações detalhadas sobre a vida privada dos indivíduos — suas redes de contatos, comportamentos, preferências, movimentos, e até mesmo pensamentos inferidos através de análise de dados — ele ganha uma capacidade sem precedentes de influenciar, manipular ou controlar esses indivíduos.

Em conclusão, enquanto a segurança pode ser uma preocupação legítima, é crucial que qualquer prática de vigilância seja realizada dentro de um quadro legal estrito, com supervisão adequada e transparência, para proteger os direitos fundamentais à privacidade e à autodeterminação. Caso contrário, a vigilância pelo poder público pode se tornar uma ferramenta de controle e opressão, em vez de proteção, o que também se aplica aos estabelecimentos de ensino.

CONSIDERAÇÕES FINAIS

Diante da problemática exposta sobre a vigilância digital, foi possível tecer ao longo dessa pesquisa, valiosas considerações sobre o tema e como ele afeta as dinâmicas da vida em sociedade. Para esse desiderato, explicou-se a necessidade de se proteger o direito à privacidade. Foi evidenciado que o direito à privacidade, como parte integrante dos direitos de personalidade, é essencial para a dignidade da pessoa humana e para o bom desenvolvimento de indivíduos autônomos e livres – indivíduos livres de pressões externas para escolherem seus próprios comportamentos.

Também foram abordados os esforços legislativos para proteger a mais nova vertente da privacidade: a proteção de dados pessoais. Em especial, tem-se a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia. No entanto, foi demonstrado que a legislação por si só não é suficiente, sendo necessário uma maior compreensão do atual cenário mundial.

A elaboração desse artigo buscou demonstrar que a vigilância digital, enquanto fenômeno global, desafia as concepções tradicionais de privacidade e requer uma abordagem multidisciplinar. Assim, foram explorados os aspectos negativos dessa vigilância, envolvendo tanto entidades privadas quanto públicas, e como ela trouxe novos paradigmas e perspectivas para o futuro da sociedade digital. Considera-se que é papel do meio acadêmico contribuir com essas e outras reflexões quanto o contexto atual para que seja garantido a formação de uma sociedade justa e livre, tendo sempre como barômetro a proteção dos direitos humanos.

REFERÊNCIAS

BOBBIO, N. **O futuro da democracia**. Rio de Janeiro: Paz e Terra, 2002.

BRASIL. **Constituição da República Federativa do Brasil de 1988**.

CASTELLS, Manuel. **A Sociedade em Rede** – a era da informação: economia, sociedade e cultura. Volume 1. São Paulo: Paz & Terra, 2002. Disponível em: <https://globalizacaoeintegracaoregionalufabc.wordpress.com/wp-content/uploads/2014/10/castells-m-a-sociedade-em-rede.pdf> Acesso em: 24 mai. 2024.

DIGITAL 2022: Global Overview Report — DataReportal – Global Digital Insights. Disponível em: <https://datareportal.com/reports/digital-2022-global-overview-report>. Acesso em: 24 mai. 2024.

DINIZ, Maria H. **Curso de direito civil brasileiro: teoria geral do direito civil**. v.1. SRV Editora LTDA, 2024. E-book. ISBN 9788553621439. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788553621439/>. Acesso em: 24 mai. 2024.

FALK, M.; RODRIGUES, R. C.O **PROBLEMA DA VIGILÂNCIA NA SOCIEDADE DA INFORMAÇÃO TECNOLÓGICA**. REDE CIDDÍ. Santa Maria/RS. 2015. Disponível em: <https://www.ufsm.br/app/uploads/sites/563/2019/09/6-15-1.pdf> Acesso em: 17 maio. 2024.

FERRAZ, T. S. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Revista da Faculdade de Direito, Universidade de São Paulo, v. 88, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231/69841> Acesso em: 17 maio de 2024

FOUCAULT, M. **Vigiar e punir**. 20. ed. Petrópolis: Vozes, 1999.

GREENWALD, G. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

JACOB NETO, Elias. **“Vigilância ou *surveillance*? Proposta para começar a compreender corretamente este fenômeno”**. Direito e Novas Tecnologias. Florianópolis: CONPEDI, 2014. p. 517 - 539. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=51c9d0385c088de7> Acesso em: 24 mai. 2024.

KANT, I. **Crítica da razão pura**. 3. ed. São Paulo: Ícone, 2021. E-book.

LYON, D. **The Electronic Eye: the rise of surveillance society**. Minneapolis: University of Minnesota Press, 1994.

Meta recebe multa de 1,2 bilhão de euros por transferência irregular de dados. Forbes, 2023. Disponível em: <https://forbes.com.br/forbes-money/2023/05/meta-recebe-multa-de-12-bilhao-de-euros-por-transferencia-irregular-de-dados/>. Acesso em: 24 maio de 2024.

MOREIRA, A. L. D.; RAZZOLINI FILHO, E.; ADRIÃO, M. C. **Vigilância do fluxo informacional e privacidade no ambiente digital**. RDBCI, Campinas, SP, v. 21, 2023. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8671505>. Acesso em: 17 maio. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948.

ORWELL, George. **1984**. Editora Alta Books, 2023. E-book. ISBN 9788578816933. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788578816933/>. Acesso em: 24 mai. 2024.

POWERFULJRE. **Joe Rogan Experience #1169 - Elon Musk**. *YouTube*. 7 de set. de 2018. Disponível em: <https://www.youtube.com/watch?v=ycPr5-27vSI&t=866s>. Acesso em: 24 mai. 2024.

PEIXOTO, E. L. C.; EHRHARDT, M. J. **BREVES NOTAS SOBRE A RESSIGNIFICAÇÃO DA PRIVACIDADE**. RBDCivil | Belo Horizonte, v. 16, p. 35-56

SARLET, I. W. **Dignidade (da pessoa) Humana e os Direitos Fundamentais na Constituição Federal de 1988**. 10. ed. Porto Alegre: Livraria do Advogado, 2015a.

SOLOVE, D. J. **The meaning and value of privacy**. Cambridge University Press, 2015. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/solove.pdf>. Acesso em: 17 maio. 2024

UNITED STATES. **USA PATRIOT Act** of 2001. Pub. L. No. 107-56, 115 Stat. 272. Disponível em: <https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>. Acesso em: 24 maio. 2024

ZUBOFF, S. **A era do capitalismo de vigilância**. Edição digital, 2021.